HP Universal CMDB Configuration Manager

per sistemi operativi Windows e Linux

Versione software: 9.20

Guida alla distribuzione

Data di rilascio della documentazione: giugno 2011

Data di rilascio del software: giugno 2011

Informazioni legali

Garanzia

Le uniche garanzie riconosciute per i prodotti e servizi HP sono stabilite nelle dichiarazioni di garanzia esplicite allegate a tali prodotti e servizi. Nulla di quanto contenuto nel presente documento potrà essere interpretato in modo da costituire una garanzia aggiuntiva. HP non è responsabile di errori e omissioni editoriali o tecnici contenuti nel presente documento.

Le informazioni contenute nel presente documento sono soggette a modifiche senza preavviso.

Legenda dei diritti riservati

Informazioni sul copyright

Aggiornamenti della documentazione

Il frontespizio di questo documento contiene le seguenti informazioni identificative:

- Data di rilascio del documento, che varia a ogni aggiornamento del documento stesso.
- Data di rilascio del software, che indica la data di rilascio di questa versione del software.

Per cercare aggiornamenti recenti o verificare che il documento utilizzato sia il più recente, visitare il sito:

http://h20230.www2.hp.com/selfsolve/manuals

Il sito richiede la registrazione come utente HP Passport per l'accesso. Per registrarsi come utente HP Passport, andare all'indirizzo:

http://h20229.www2.hp.com/passport-registration.html

In alternativa, fare clic sul collegamento **New users - please register** sulla pagina di accesso di HP Passport.

Sottoscrivendo lo specifico servizio di assistenza prodotti, sarà inoltre possibile ricevere edizioni aggiornate o nuove. Per ulteriori dettagli, contattare il rappresentante commerciale di HP.

Assistenza

Visitare il sito Web dell'Assistenza HP Software all'indirizzo:

http://www.hp.com/go/hpsoftwaresupport

Questo sito Web fornisce informazioni di contatto e dettagli su prodotti, servizi e assistenza offerti da HP Software.

L'assistenza online di HP Software offre al cliente la possibilità di risolvere autonomamente alcuni problemi. Costituisce un modo rapido ed efficiente per accedere agli strumenti interattivi di assistenza tecnica necessari per la gestione dell'azienda. Per i clienti dell'assistenza, il sito Web offre i seguenti vantaggi:

- Ricerca di documenti nelle Knowledge Base
- Invio e consultazione di casi di assistenza e richieste di miglioramenti
- Download di patch software
- Gestione di contratti di assistenza
- Ricerca di recapiti di assistenza HP
- Consultazione delle informazioni relative ai servizi disponibili
- Partecipazione a forum di discussione con altri utenti del software
- Ricerca e iscrizione a eventi di formazione software

La maggior parte delle aree di assistenza richiede la registrazione come utente HP Passport per l'accesso. In molti casi è inoltre necessario un contratto di assistenza. Per ottenere un ID di HP Passport, andare all'indirizzo:

http://h20229.www2.hp.com/passport-registration.html

Per ulteriori informazioni sui livelli di accesso, visitare:

http://h20230.www2.hp.com/new_access_levels.jsp

Sommario

PARTE I: INSTALLAZIONE E CONFIGURAZIONE

PARTE II: APPENDICI

Parte I

Installazione e configurazione

1

Panoramica

Questo capitolo comprende:

Componenti

HP Universal CMDB Configuration Manager è un rilascio congiunto di diversi componenti:

- **HP Universal CMDB foundation**

  HP Universal CMDB foundation (UCMDB foundation) è un database per la gestione delle configurazioni (CMDB) per le organizzazioni IT enterprise per documentare, archiviare e gestire le definizioni dei servizi di business e le relazioni associate all'infrastruttura.

  UCMDB foundation implementa un modello di dati, gestione del flusso dati e funzionalità di modellazione dei dati, offre inoltre l'analisi di impatto, tracciatura dei cambiamenti e funzionalità di reporting per poter trasformare i dati CMDB in informazioni comprensibili e eseguibili che aiutano a rispondere a domande critiche e nella risoluzione dei problemi di business.

- **HP Universal CMDB Configuration Manager**

  HP Universal CMDB Configuration Manager (Configuration Manager) introduce nuove topologie basate sui criteri e una nuova governance di configurazione dell'inventario. Creato appositamente per i gestori delle configurazioni e i proprietari delle configurazioni, consente a questi utenti di effettuare analisi in aggiunta ai dati CI e contenuti della topologia disponibili in o tramite UCMDB. Configuration Manager fornisce ai gestori e proprietari delle configurazioni gli strumenti necessari per impostare in modo semplice i criteri di configurazione sia per la topologia che per l'inventario, così come la determinazione automatica dei loro livelli di conformità agli standard organizzativi.

  Configuration Manager è distribuito come server aggiuntivo Tomcat. Comunica con il server UCMDB utilizzando un UCMDB SDK estensivo.

- **HP Discovery e Dependency Mapping Advanced Edition**

  Il software HP Discovery e Dependency Mapping Advanced Edition (DDMA), grazie ai contenuti ricchi e costantemente aggiornati, rappresenta il metodo preferito da UCMDB per l'acquisizione e la manutenzione dei dati dell'infrastruttura IT.

- **HP Operations Orchestration**

  HP Operations Orchestration (OO) è uno strumento per l'authoring e la distribuzione del flusso. Le funzionalità trascina e collega in OO Studio consentono agli utenti di progettare, creare, condividere e personalizzare i flussi anche a utenti con competenze di programmazione minime o nulle. OO Studio supporta la collaborazione tra più autori tramite le funzionalità di controllo della versione. Il potente debugger integrato consente di eseguire i test dei flussi su più ambienti accelerando la distribuzione dei contenuti e consentendo la convalida dei flussi per un'esecuzione stabile e attendibile.-

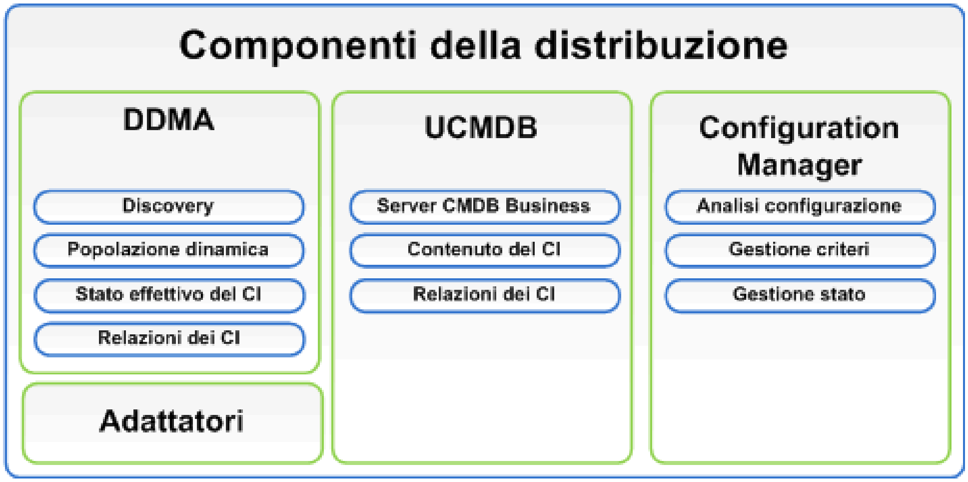
  OO Studio consente inoltre agli utenti di distribuire in modo semplice i flussi. OO Studio consente agli utenti di confrontare e promuovere i flussi attraverso più ambienti (sviluppo, test, gestione temporanea e produzione). I processi standard possono essere documentati e la documentazione strutturata può essere generata in modo da supportare i requisiti di conformità utilizzando Studio.

- **Integrazione Configuration Manager-OO**

  Configuration Manager offre la possibilità di eseguire i flussi OO dal framework di Configuration Manager. I flussi OO possono essere eseguiti principalmente in due modi;

  - **Integrazione processo** – consente di aprire un RFC in una richiesta service desk esterna che allinea un CI specifico con un criterio di configurazione specifico.

- **Monitoraggio e aggiornamento criteri** – consente di attivare un flusso OO per monitorare e aggiornare il problema di configurazione. Ad esempio, è possibile allocare ulteriore memoria su un computer host virtuale.



Identificare l'ambiente

Questa guida descrive il processo di distribuzione di HP Universal CMDB Configuration Manager da diversi punti di partenza possibili:

Per Configuration Manager

- Se è installato Configuration Manager versione 9.10

  Per i dettagli relativi all'aggiornamento di Configuration Manager alla versione corrente, consultare "Aggiornamento di Configuration Manager" a pagina 41.

- Se non è installata la versione di Configuration Manager

  Per informazioni, consultare una delle seguenti:

  - "Installazione di HP Universal CMDB Configuration Manager su una piattaforma Windows" a pagina 19
  - "Installazione di HP Universal CMDB Configuration Manager su una piattaforma Linux" a pagina 45

Per UCMDB

- Se è installata una versione di UCMDB precedente alla 9.03

  Procedere come segue:

  - Eseguire l'aggiornamento a UCMDB versione 9.03. Per informazioni, consultare *HP Universal CMDB Deployment Guide* in PDF. È possibile scaricare il manuale da www.hp.com/go/hpsoftwaresupport.
  - Installare il Cumulative Update Pack 2. È possibile ottenerlo dal supporto di installazione di Configuration Manager o scaricandolo da www.hp.com/go/hpsoftwaresupport.

  Per informazioni sulla configurazione della conformità enterprise, consultare "Configurare il database o lo schema utenti" a pagina 20.

- Se è installato UCMDB versione 9.03

  Installare il Cumulative Update Pack 2. È possibile ottenerlo dal supporto di installazione di Configuration Manager o scaricandolo da www.hp.com/go/hpsoftwaresupport.

  Per informazioni sulla configurazione della conformità enterprise, consultare "Configurare il database o lo schema utenti" a pagina 20.

- Se non è installata una versione di UCMDB

  Procedere con una delle seguenti operazioni:

  - Usare Gestione distribuzione (solo per sistemi Windows) per installare UCMDB durante l'installazione di Configuration Manager. Per informazioni, consultare "Installazione di HP Universal CMDB Configuration Manager su una piattaforma Windows" a pagina 19.
  - Installare Configuration Manager su un sistema Linux seguendo le istruzioni in "Installazione di HP Universal CMDB Configuration Manager su una piattaforma Linux" a pagina 45.

Informazioni generali

Questa guida tiene in considerazione anche le distribuzioni speciali di UCMDB che si possono avere in un ambiente (ad esempio, distribuzione con disponibilità elevata) e consente di apportare le variazioni necessarie alla procedura di distribuzione per tali distribuzioni.

Nota: è supportata l'installazione di UCMDB e Configuration Manager sullo stesso server. Per la scalabilità in un ambiente di produzione, HP Software consiglia l'installazione di questi componenti su server diversi.

L'uso di Configuration Manager richiede la configurazione di UCMDB con una modalità schema consolidata e la creazione di un nuovo stato di UCMDB (stato Autorizzato). Queste configurazioni vengono eseguite automaticamente durante la procedura di distribuzione in entrambi i tipi di installazione (sia l'installazione di un UCMDB esistente, sia nel caso venga installato tramite Gestione distribuzione).

Importante: facendo riferimento a una installazione di UCMDB esistente con uno schema non ancora consolidato, la fase di consolidamento potrebbe richiedere del tempo (da 20 a 60 minuti) per database molto popolati (quelli che contengono più di 5 milioni di CI).

Se si sta distribuendo solo Configuration Manager (utilizzando una installazione esistente o aggiornata di UCMDB), il server UCMDB deve essere in esecuzione per completare l'installazione di Configuration Manager.

Matrice di supporto

Requisiti di sistema del server

CPU	Almeno 4 core
Memoria (RAM)	Almeno 4 GB
Piattaforma	x64
Sistema operativo	Windows (64-bit) ➤ Windows 2003 Enterprise SP2 e R2 SP2 ➤ Windows 2008 Enterprise SP2 e R2 Linux ➤ Red Hat Enterprise Linux x86 (64-bit)
Database	➤ Microsoft SQL Server 2005 SP2; 2005 Compatibility Mode 80 (Enterprise Edition in tutti i casi) ➤ Microsoft SQL Server 2008 ➤ Oracle 10.2.x, 11.x
Server Web	➤ Microsoft IIS 7 ➤ Apache 2
HP Universal CMDB	➤ HP Universal CMDB versione 9.03 con CUP 2 (installazione tipica di CMDB) Per un elenco completo dei requisiti di sistema, fare riferimento a *HP Universal CMDB Deployment Guide* in PDF. **Nota:** ➤ Quando il server HP Universal CMDB è distribuito in combinazione con Configuration Manager, sono necessari l'Enterprise Edition di Oracle e l'opzione Oracle Partitioning. ➤ Se il server HP Universal CMDB è stato distribuito in precedenza con la Standard Edition di Oracle, e si desidera aggiungere Configuration Manager all'installazione, è necessario prima convertire il database Standard Edition in un database Enterprise Edition con l'opzione Partitioning abilitata.

LDAP (facoltativo)	➤ Active Directory ➤ SunONE 6.x
Dimensione minima consigliata per lo schema del database (facoltativa)	2 GB

Requisiti del client

Sistema operativo	➤ Windows XP x86 (32-bit) ➤ Windows Vista x86 (32-bit e 64-bit) ➤ Windows 7 x86 (32-bit e 64-bit)
Browser	➤ Microsoft Internet Explorer 7.0, 8.0 ➤ Mozilla Firefox 3.x, 4
Plug-in Flash Player del browser	Flash Player 9 o versione successiva **Nota:** scaricare Flash Player da: http://www.adobe.com/products/flashplayer/.
Risoluzione schermo	➤ 1024x768 minima ➤ 1280x1024 consigliata
Qualità colori	Almeno 16 bit

HP Operations Orchestration (facoltativo)

HP Operations Orchestration	➤ 7.51, 9.0

2

Installazione di HP Universal CMDB Configuration Manager su una piattaforma Windows

Importante: Consultare le note sulla versione per le procedure di installazione più aggiornate.

Questo capitolo comprende:

Impostazione di pre installazione

Questa sezione comprende:

Configurare il database o lo schema utenti

Nota: questa attività viene eseguita automaticamente come parte del processo di installazione di Configuration Manager; tuttavia, è anche possibile eseguirla manualmente.

Per lavorare con Configuration Manager, è necessario specificare uno schema database. Configuration Manager e UCMDB utilizzano schemi diversi. Configuration Manager supporta Microsoft SQL Server e Oracle Database Server. Questa attività descrive come creare uno schema per Configuration Manager. Se si installa UCMDB, sarà necessario impostare un database separato e un schema utente anche per esso. Per informazioni, consultare *HP Universal CMDB Deployment Guide* in PDF.

Nota: Per i requisiti di sistema di Microsoft SQL Server e Oracle Server consultare "Requisiti di sistema del server" a pagina 16.

Per configurare il database:

1 Allocare un database di Microsoft SQL Server oppure uno schema utenti di Oracle Server.

➤ Per **Microsoft SQL Server**: attivare l'isolamento istantanea.

Una volta creato il database, eseguire il seguente comando:

```
alter database <nome_database_ccm> set read_committed_snapshot on
```

Per ulteriori informazioni sulla funzionalità di isolamento istantanea di SQL Server, consultare http://msdn.microsoft.com/en-us/library/tcbchxcb(VS.80).aspx.

➤ Per **Oracle**: concedere all'utente Oracle solo i ruoli **Connect** e **Resource**. (concedendo i privilegi **Select any table** la procedura di popolazione dello schema restituisce un errore.)

2 Verificare le seguenti informazioni, necessarie durante la procedura di configurazione:

✔	**Informazioni necessarie**
	Nome host e porta DB
	Nome utente e password DB
	Per MS SQL: Nome database
	Per Oracle: SID

Installazione di Configuration Manager in un ambiente UCMDB a disponibilità elevata

Per utilizzare Configuration Manager in un ambiente UCMDB a disponibilità elevata, continuare con i seguenti passaggi:

1 Spegnere il server di backup (passivo). Una volta spento, attendere due minuti.

2 Installare Configuration Manager versione 9.20.

a Utilizzare i dettagli dell'host di bilanciamento del carico.

b Installare Configuration Manager su un terzo server, non sui server UCMDB.

3 Verificare che UCMDB e Configuration Manager funzionino correttamente.

4 Avviare il server di backup (passivo) per avere Disponibilità elevata.

Nota: La modalità Disponibilità elevata non è supportata dallo stesso HP Universal CMDB Configuration Manager 9.20.

Installare Configuration Manager

Gestione distribuzione può installare UCMDB, Configuration Manager e DDMA in diverse configurazioni (scelte e configurate nella pagina Selezione prodotti della procedura di installazione):

- ➤ Installazione di una nuova istanza di UCMDB
- ➤ Installazione di una nuova istanza di Configuration Manager e collegamento a una nuova istanza o a una istanza esistente di UCMDB
- ➤ Integrazione di una nuova istanza di Configuration Manager con una istanza esistente di OO
- ➤ Installazione di istanze multiple di DDMA

Nota:

- ➤ Gestione distribuzione offre la possibilità di installazione prodotti, componenti e integrazioni su un computer di destinazione. Gestione distribuzione non supporta la disinstallazione di prodotti, la modifica di prodotti e l'installazione di patch su un prodotto installato, pertanto deve essere eseguita manualmente.
- ➤ Una volta premuto il pulsante **Next** nella pagina Selezione prodotto, non è possibile tornare alla pagina precedente e selezionare nuovamente la configurazione di distribuzione. Nel caso sia necessario apportare delle modifiche alla configurazione di distribuzione, riavviare la Gestione distribuzione.

Per installare Configuration Manager:

1. Per avviare l'installazione, inserire il supporto di installazione di Configuration Manager nel computer e individuare il file **setup.exe**.
2. Fare doppio clic sul file **setup.exe** per eseguire Gestione distribuzione.
3. Disabilitare il firewall di Windows sul computer di destinazione per tutta la durata dell'installazione. Per informazioni relative al firewall, consultare il passaggio 6 in questa procedura.

4 Accettare il Contratto di licenza con l'utente finale e fare clic su **Next** per aprire la pagina Selezione prodotto.

Nota: I termini del contratto di licenza si applicano a tutti i prodotti selezionati nella pagina Selezione prodotto di Gestione distribuzione.

---

5 Nella pagina Selezione prodotto, selezionare tutti i prodotti per la distribuzione. Una volta terminato, fare clic su **Next** per passare alla pagina Posizione server.

La pagina Selezione prodotto consente di selezionare i prodotti da installare e di specificare le opzioni di configurazione eseguite durante la distribuzione.

a Selezionare un'opzione di installazione di HP Universal CMDB foundation.

Sono disponibili due opzioni per l'installazione di UCMDB foundation:

- **Connetti a un server esistente** – quando selezionata, questa opzione connette e configura Configuration Manager o Discovery and Dependency Mapping ad una istanza esistente di un server UCMDB foundation.

Nota: La versione di UCMDB su un server esistente deve essere la versione 9.03 con CUP 2 o versione successiva.

- **Installa nuovo server** – quando selezionata, questa opzione installa, configura e connette a una nuova istanza del server di UCMDB foundation, e configura e connette Configuration Manager o DDMA alla nuova istanza del server UCMDB foundation.

b Selezionare la casella di controllo **Configuration Manager** per installare e configurare una nuova istanza di Configuration Manager.

Se desiderato, selezionare **Connetti a una istanza HP Operation Orchestration esistente**. Questa opzione configura un'integrazione tra Configuration Manager e Operations Orchestration popolando Configuration Manager con i dettagli relativi alla connessione al server OO.

c **HP Discovery e Dependency Mapping Advanced Edition.** Quando selezionata, questa opzione installa e configura nuove istanze dei DDMA.

L'opzione **Numero di istanze DDMA** consente di installare più istanze di DDMA. Il numero specificato nel campo input indica il numero di istanze di DDMA connesse a una singola istanza del server UCMDB.

Nota: Gestione distribuzione supporta distribuzioni multiple di istanze DDMA nella stesso DMZ. Gestione distribuzione supporta un massimo di 10 istanze di probe di individuazione in ciascuna distribuzione. Nel caso siano necessari altri probe di individuazione, installarli in più fasi di distribuzione in gruppi di dieci.

---

6 Specificare la posizione dei server remoti e le credenziali dei computer di distribuzione di destinazione per ciascun prodotto selezionare per la distribuzione nella pagina Posizione server. Una volta terminato, fare clic su **Next** per passare alla pagina Connessioni.

Opzioni di distribuzione

Selezionare un'opzione di distribuzione per la posizione di destinazione. Sono disponibili due opzioni:

- **Distribuisci sul computer locale** – utilizzare questa opzione per la distribuzione di un prodotto sullo stesso computer di Gestione distribuzione. In questo caso, i campi dei dettagli relativi all'host remoto e le credenziali sono disabilitati.
- **Distribuisci sul seguente computer** – quando selezionata, è necessario specificare l'indirizzo dell'host remoto e i dettagli del sistema operativo. Le credenziali utente specificate devono disporre dei privilegi di amministrazione sull'host remoto.

Nota: Quando si assegna un nome host per la distribuzione di un prodotto, utilizzare esclusivamente le lettere (a-z), le cifre (0-9) e il segno meno ('-').

Le informazioni di seguito sono importanti quando si specificano i dettagli relativi al computer remoto:

- **Protocolli WMI e SMB** – utilizzati per la connessione al computer remoto. I prerequisiti di seguito devono esistere per far si che Gestione distribuzione si connetta al computer remoto.
  - **Servizio WMI** – il servizio WMI deve essere in esecuzione sul computer remoto.
  - **Servizio server** – per abilitare il protocollo SMB, il Servizio server deve essere in esecuzione sul computer remoto.

- **Firewall di Windows** – il computer remoto deve consentire le connessioni amministratore da remoto. Eseguire il comando pertinente nella console del prompt di comandi sul computer remoto:

Sistema operativo	Comando
Windows XP Windows Server 2003 Windows Server 2003 R2	netsh firewall set service RemoteAdmin enable
Windows Vista Windows 7 Windows Server 2008 Windows Server 2008 R2	netsh advfirewall firewall set rule group="windows management instrumentation (WMI)" new enable=Yes

Test connessione

Fare clic su **Test connessione** per verificare che le credenziali di connessione e i dettagli siano corretti e per analizzare le risorse di sistema locali e remote.

Se il test della connessione ha esito negativo, Gestione distribuzione visualizza un messaggio di errore con i dettagli. Premendo il pulsante **Next**, viene forzata automaticamente la verifica del test di connessione.

La convalida delle risorse del computer viene eseguita su:

- **Piattaforma sistema operativo** – verifica che il sistema operativo sia certificato per la distribuzione del prodotto.
- **Spazio su disco** – verifica che lo spazio su disco sia sufficiente.
- **Memoria** – verifica che la memoria fisica sia sufficiente.
- **Porte** – verifica che le porte richieste siano disponibili.

La convalida delle risorse eseguita tramite il test della connessione varia in relazione alle matrici di prodotto supportate.

Nota: Se il test restituisce un errore **Sconosciuto**, verificare che i seguenti servizi siano in esecuzione sul computer host di distribuzione:

➤ Server

➤ Strumentazione gestione Windows

Verificare che il controllo account utente (UAC) sia disattivato prima di fare clic su **Next**. Per informazioni su UAC, andare su http://technet.microsoft.com/en-us/library/cc709691(WS.10).aspx.

7 Configurare le connessioni tra i prodotti selezionati nella pagina Connessioni. Le opzioni di connessione visualizzate nella pagina Connessioni riflettono i componenti selezionati per la distribuzione nella pagina Selezione prodotto. Una volta terminato, fare clic su **Next** per passare alla pagina Configurazione installazione.

➤ Integrazione di UCMDB con Configuration Manager

Questa sezione viene visualizzata quando si sceglie di installare Configuration Manager con l'opzione **Connetti a un server esistente** e consente di configurare l'integrazione di Configuration Manager con UCMDB.

Nota: per poter eseguire la connessione con un'istanza esistente di UCMDB, è necessario installare UCMDB versione 9.03 con CUP 2 o versione successiva.

Specificare i seguenti dettagli di UCMDB:

Campo	Definizione
Nome host/IP di UCMDB	Indirizzo posizione della distribuzione di UCMDB. ➤ Se UCMDB è configurato in modalità disponibilità elevata, seguire le istruzioni in "Installazione di Configuration Manager in un ambiente UCMDB a disponibilità elevata" a pagina 21. ➤ Se UCMDB è installato sul computer locale e Configuration Manager è installato su un computer remoto, il nome dell'istanza di UCMDB locale deve essere FQDN e non localhost. ➤ Se UCMDB e Configuration Manager ha nomi dominio DNS diversi ed è necessaria l'integrazione LW-SSO, è necessario specificare l'FQDN nel campo di input dell'host UCMDB esistente.
Protocollo	Protocollo HTTP o HTTPS.
Porta UCMDB HTTP(S)	I valori predefiniti per la porta HTTP o HTTPS sono **8080** per HTTP e **8443** per HTTPS.
File certificato client	Questo campo viene visualizzato quando è selezionato il protocollo HTTPS. È necessario posizionare manualmente il file certificato del client UCMDB nell'host di destinazione di Configuration Manager e specificare il percorso completo del file incluso il nome del file nel campo di input vicino. Se UCMDB utilizza HTTPS allora è necessario utilizzare lo scambio di chiave. Lo scambio di chiave non viene convalidato durante il test della connessione.

Campo	Definizione
Nome cliente	Il nome cliente predefinito di UCMDB è **Client predefinito**. Il valore del nome cliente viene utilizzato durante la configurazione dell'integrazione tra UCMDB e Configuration Manager. Questo valore non viene convalidato dal test della connessione. La distribuzione ha esito negativo qualora venga specificato un valore errato.
Porta JMX	Il valore predefinito è **29601**.
Utente sistema UCMDB (JMX)	L'utente sistema UCMDB (JMX) viene utilizzato per l'attivazione delle funzioni JMX, ad esempio la creazione di un utente integrazione di Configuration Manager e la distribuzione del pacchetto di Configuration Manager. Il valore predefinito è **sysadmin**.
Password sistema UCMDB	La password utente di sistema di UCMDB. Il valore predefinito è **sysadmin**.

Nota: Configuration Manager è configurato con un repository utente interno. Per utilizzare un LDAP esterno come repository utente, è necessario configurare Configuration Manager per utilizzarlo. Per informazioni, consultare "Impostazioni di sistema" nella *Guida dell'utente di HP Universal CMDB Configuration Manager*.

➤ Integrazione di Configuration Manager con OO

Questa sezione viene visualizzata quando si seleziona l'opzione **Connetti a una istanza HP Operation Orchestration esistente** e consente di configurare l'integrazione di Configuration Manager con OO.

Specificare i seguenti dettagli di OO:

Campo	Definizione
Versione OO	Le versioni di OO valide sono 7.5 e 9.0.
Nome host/IP di OO	L'host o l'indirizzo IP del computer server OO.
Numero porta OO	Il numero porta predefinito è **8443**.
Nome utente OO	Il nome utente OO predefinito è **admin**. In OO l'utente deve essere configurato come esterno.
Password OO	Il password OO predefinita è **admin**.

➤ Configurazione di DDMA

I campi di seguito vengono visualizzati quando si seleziona l'opzione **Istanza Discovery and Dependency Mapping Advanced Edition** e consente di configurare una connessione DDMA verso UCMDB.

Specificare i seguenti dettagli di DDMA:

Campo	Definizione
Identificatore probe flusso dati	Il valore predefinito è il nome host del computer DDMA. Il campo viene popolato automaticamente. Il valore può essere cambiato.
Usa dominio predefinito	Questa opzione è selezionata per impostazione predefinita e influisce sul valore del nome dominio. Deselezionando la casella di controllo, è possibile cambiare il nome predefinito su un valore diverso.
Nome dominio	Il valore predefinito è impostato su **DefaultDomain**. Deselezionare la casella di controllo **Usa dominio predefinito** per abilitare il campo.

Campo	Definizione
Dimensioni heap iniziali in MB	La dimensione iniziale della memoria assegnata al JVM di DDMA. Il valore predefinito è 256 MB.
Dimensioni heap massime in MB	La dimensione massima della memoria assegnata al JVM. Il valore predefinito è 512MB.

8 Impostare i dettagli della directory di destinazione della distribuzione per le distribuzioni dei prodotti selezionati nella pagina Configurazione installazione. Una volta terminato, fare clic su **Next** per passare alla pagina Configurazione database.

Per ciascun prodotto selezionato viene fornito un percorso directory predefinito. Nel caso di una distribuzione su un computer locale, è disponibile l'opzione Sfoglia per selezionare un percorso directory diverso. Nel caso di installazione su un computer remoto, questa opzione è disabilitata.

Nota: la directory di installazione non può contenere spazi all'interno del nome, possono essere utilizzati esclusivamente lettere inglesi (a-z), cifre (0-9) e il segno meno ('-').

---

9 Configurare ciascuna connessione database e schema database del prodotto nella pagina Configurazione database. Una volta terminato, fare clic su **Next** per passare alla pagina Configurazione porte.

È possibile configurare i seguenti database (schemi):

➤ Schema UCMDB-CM

➤ Schema UCMDB

➤ Schema cronologia UCMDB

Campo	Definizione
Nome host/IP database	L'indirizzo di ubicazione del server del database.
Porta	MSSQL e Oracle utilizzano porte predefinite diverse. La porta database predefinita di Oracle è 1521, mentre la porta database di MSSQL è 1433.
SID (Oracle)	Il nome istanza del database Oracle.
Nome utente amministratore (Oracle)	Immettere il nome utente amministratore di Oracle in relazione al server Oracle.
Password amministratore (Oracle)	Immettere la password amministratore di Oracle in relazione al server Oracle.
Test connessione	Esegue il test della connessione sull'host del DB di destinazione, utilizzando le credenziali specificate.
Nome schema (Oracle)	Immettere il nome dello schema.
Password schema (Oracle)	Immettere la password dello schema. Questo campo viene visualizzato quando si crea un nuovo schema
Spazio tabella predefinito (Oracle)	Immettere il nome dello spazio tabella predefinito.
Spazio tabella temporaneo (Oracle)	Immettere il nome dello spazio tabella temporaneo.
Nome database (MSSQL)	Immettere il nome dello schema database da usare/creare nel server MSSQL.
Nome utente database (MSSQL)	Immettere il nome utente amministratore di MSSQL in relazione al server MSSQL.
Password database (MSSQL)	Immettere la password amministratore di MSSQL in relazione al server Oracle.

Nota:

- Nel caso lo spazio tabella di UCMDB sia completo, la distribuzione del prodotto verrà eseguita ma i prodotti e i componenti non funzioneranno correttamente
- Non è supportata la creazione di un nuovo schema UCMDB e la connessione a uno schema cronologia di UCMDB esistente.
- Non è supportato, per ragioni legate alla protezione, l'uso dell'autenticazione NTLM durante la configurazione di schemi di UCMDB con un database MSSQL quando UCMDB è installato da remoto. Se è necessaria l'autenticazione NTLM, distribuire UCMDB localmente.

Modalità schema

Configuration Manager richiede la configurazione di UCMDB con una modalità schema consolidata e la creazione di un nuovo stato di UCMDB.

Facendo riferimento a una installazione di UCMDB esistente con uno schema non ancora consolidato, la fase di consolidamento automatico potrebbe impiegare del tempo (da 20 a 60 minuti) per database molto popolati (quelli che contengono più di 5 milioni di CI).

Nota: le connessioni Oracle Real Application Cluster (RAC) e SQL Server NTLM non sono supportate come parte dell'installazione. Se queste connessioni sono necessarie, per prima cosa installare Configuration Manager con una connessione database semplice e, una volta completata l'installazione, cambiare la connessione dalla configurazione prodotto specifico. Per fare ciò, modificare il file **database.properties** in relazione alle specifiche del database. Per informazioni, consultare "Configurazione database avanzata (per Configuration Manager)" a pagina 34.

Modalità configurazione database

Configuration Manager e UCMDB devono utilizzare schemi diversi.

Configuration Manager consente all'utente di configurare ciascun database sia su un server database Oracle che MSSQL.

Tipi di configurazioni

È possibile sia connettersi a uno schema esistente che creare un nuovo schema. La connessione a uno schema esistente ne sovrascrive i contenuti.

Configurazione database

Questa procedura viene eseguita automaticamente da Gestione distribuzione. Per eseguire la procedura manualmente, consultare "Configurare il database o lo schema utenti" a pagina 20.

Configurazione database avanzata (per Configuration Manager)

È necessario configurare una connessione al database associata con una connessione URL standard. Nel caso siano necessarie funzionalità avanzate, ad esempio Oracle Real Application Cluster, impostare una connessione standard, quindi modificare manualmente il file **database.properties** per configurare le funzionalità avanzate.

Configuration Manager utilizza driver nativi sia per i database Oracle che Microsoft SQL Server. Sono supportate tutte le funzionalità dei driver nativi, posto che queste funzionalità possano essere configurate utilizzando l'URL del database. L'URL si trova nel file **database.properties**.

Terminata la procedura guidata di Gestione distribuzione, possono essere eseguite ulteriori configurazioni di database schemi.

Campi configurazione database

Sono disponibili due tipi di database – Oracle e MSSQL. I campi di input cambiano in relazione al tipo di database selezionato.

10 Specificare le porte di connessione di Configuration Manager nella pagina Configurazione porte. Una volta terminato, fare clic su **Next** per passare alla pagina Configurazione utenti.

Configuration Manager fornisce delle impostazioni predefinite per le porte che vengono visualizzate nei campi di input nella pagina della procedura guidata Configurazione porte.

Se un numero di porta è in conflitto con una installazione esistente, consultare il responsabile IT prima di cambiare il numero della porta.

Campo	Definizione
Porta HTTP applicazione	8180
Porta HTTP JMX	39900
Porta Tomcat	8005
Porta AJP	8009 (Apache Java Protocol)
Porta HTTPS applicazione	8143
Porta remota JMX	39600

Fare clic sul pulsante **Reimposta valori predefiniti** per ripristinare le porte ai valori predefiniti specificati da Gestione distribuzione.

11 Creare i seguenti utenti nella pagina Configurazione utenti:

- Istanza utente di accesso iniziale di UCMDB-CM con autorizzazioni amministratore.
- Utente di integrazione in UCMDB - un utente di integrazione viene creato in UCMDB su richiesta da Configuration Manager per supportare l'integrazione tra questi due prodotti.

Una volta terminato, fare clic su **Next** per passare alla pagina Configurazione protezione.

12 Attivare Global LW-SSO su una nuova istanza di UCMDB e Configuration Manager nella pagina Configurazione protezione. LW-SSO è configurato solo su nuove istanze di Configuration Manager o UCMBD, in relazione alla scelta fatta nella pagina Selezione prodotto. Una volta terminato, fare clic su **Next** per passare alla pagina Riepilogo.

LW-SSO è un framework modulare utilizzato per convalidare diversi tipi di autenticazioni e token di protezione token (ad esempio LW-SSO e SAML2). LW-SSO viene utilizzato per collegare e sfruttare le informazioni automaticate da ambienti diversi nei contesti di protezione dell'applicazione all'interno di un'applicazione o framework di protezione.

La configurazione LW-SSO è diversa in relazione ai componenti del prodotto selezionati.

Nella connessione di Configuration Manager a una istanza di UCMDB o OO esistente, LW-SSO è configurato solo su Configuration Manager. È necessario estrarre la stringa di LW-SSO da UCMDB o OO, e inserire questa stringa nel campo di input Stringa di LW-SSO. Nella connessione a UCMDB e OO, certificare che le stringhe LW-SSO definite nelle istanze di UCMDB e OO corrispondano.

Nella connessione a una nuova istanza di Configuration Manager a una istanza esistente di UCMDB, usare FQDN come nome host di UCMDB.

Per estrarre la stringa di LW-SSO da UCMDB:

a Aprire UCMDB e selezionare **Amministrazione** > **Gestione impostazioni infrastruttura**.

b Nella colonna **Nome**, selezionare e fare doppio clic sul campo stringa di inizializzazione di LW-SSO.

c Copiare la stringa dal campo Valore corrente.

d Incollare il valore nel campo Stringa LW-SSO nella pagina Configurazione protezione.

Nella connessione di Configuration Manager a una nuova istanza di UCMDB, LW-SSO viene configurato automaticamente su UCMDB così come su Configuration Manager.

13 Riesaminare le impostazioni di installazione e configurazione nella pagina Riepilogo. Una volta terminato, fare clic su **Next** per passare alla pagina Convalida.

La pagina Riepilogo riassume tutti i dettagli della configurazione e le immissioni dell'utente. È possibile revisionare il contenuto del riepilogo, se necessario, facendo clic sul pulsante Indietro nelle pagine fino a raggiungere la pagina desiderata, e regolare quindi le impostazioni di distribuzione. Tornare alla pagina Riepilogo facendo clic su **Next** come necessario.

14 Gestione distribuzione esegue quindi una serie di azioni per verificare che le risorse di sistema dei computer remoti siano sufficienti, che le immissioni dell'utente siano corrette e convalida le impostazioni di configurazione del database. Queste convalide indicano se le impostazioni di definizione dell'utente sono conformi alle limitazioni ambientali note. Il processo di convalida si avvia automaticamente, oppure, se si è tornati a una pagina precedente in Gestione distribuzione e sono state apportate modifiche alla configurazione, fare clic su **Esegui convalida** per avviare il processo di convalida. Una volta terminato, fare clic su **Distribuisci** per passare alla pagina Distribuzione.

15 La pagina Distribuzione riflette lo stato del processo di distribuzione durante l'avanzamento. Il processo di distribuzione include le installazioni dei prodotti, le procedure di avvio e le rispettive integrazioni e connessioni con altri prodotti.

Il processo di distribuzione è completo una volta che tutti i prodotti sono stati avviati.

Fare clic su **Dettagli** per visualizzare i dettagli dell'avanzamento della distribuzione, comprese le procedure eseguite da Gestione distribuzione per ciascuna distribuzione di prodotto selezionata.

Fare clic su **Annulla** per annullare normalmente la distribuzione, consentendo all'azione di distribuzione corrente di essere completata prima di interrompere la distribuzione.

Fare clic su **Interrompi** (disponibile solo dopo aver fatto clic su **Annulla**) per terminare in modo forzato l'azione corrente e la distribuzione. L'interruzione della distribuzione può causare uno stato non determinato dei prodotti.

Conferme

La tabella di seguito fornisce un elenco delle convalide eseguite tramite Gestione distribuzione.

Conferma	Messaggio di errore	Descrizione
Verifica credenziali di accesso	Credentials verification failed	Le credenziali utente specificate non sono corrette.
		Impossibile stabilire la connessione.
Verifica compatibilità sistema operativo	Target operating system platform is <Piattaforma> Product <Nome prodotto> supports the following platforms <Platform>	Il sistema operativo di destinazione effettivo non corrisponde all'elenco dei sistemi operativi certificati per il prodotto.
Verifica memoria	The assigned memory (<Memoria> MB) exceeds the available memory (<Memoria> MB) on <Target>	Memoria nel computer di destinazione insufficiente per tutti i prodotti assegnati
	<Memoria> MB of memory are verified to be available on <computer di destinazione>	Convalida eseguita.
Verifica spazio su disco	assigned disk space for (<Memoria> MB) exceeds available disk space (<Memoria> MB) on drive <Target>	Spazio su disco nel computer di destinazione insufficiente per tutti i prodotti assegnati.
	<Memoria> MB of disk space are verified to be available on drive <di destinazione>	Convalida eseguita.

Conferma	Messaggio di errore	Descrizione
Verifica che tutte le proprietà obbligatorie sono state specificate	Missing the target storage device for the product: <destinazione>	La directory di installazione del prodotto non è impostata.
Verifica che tutti i computer di distribuzione sono definiti	No deployment machine is defined for <nome prodotto>	Il prodotto non è configurato per essere distribuito su un computer.
Verifica credenziali di accesso	Credentials verification failed	Credenziali di accesso errate.
Verifica che UAC è disabilitato	The UAC is enabled	L'UAC è abilitato sul computer di destinazione.
Verifica porte libere	The required port number <Porta> is already in use on <destinazione>	La porta richiesta sul computer di destinazione è già in uso.
Verifica esistenza del dispositivo di archiviazione di destinazione	The target storage device <dispositivo> does not exist on <destinazione>	Il dispositivo di archiviazione di destinazione selezionato non esiste sul computer di destinazione.
Convalida esistenza schema	Schema <nome> does not exist/ already exist	Lo schema sul computer di destinazione esiste/non esiste.
Convalida esistenza autorizzazione schema	Validate <autorizzazioni> schema tables user permissions existence	L'utente DB non dispone di autorizzazioni sufficienti
Convalida esistenza tabelle schema	Schema Tables <tabelle> on the database: <Tabelle> already exist	Le tabelle schema sul database esistono già.
Convalida esistenza autorizzazioni utente tabelle schema	The database user does not have the correct permissions	L'utente database non dispone delle autorizzazioni corrette.

Conferma	Messaggio di errore	Descrizione
Verifica connessione UCMDB	Connection failed. Connection to UCMDB failed, host: <Host>, username: <Nome utente>, port: <Porta>, protocollo: <Protocollo> due to <Errore>	Test connessione a UCMDB con le impostazioni di connessione specificate non riuscito.
	Existing UCMDB version must be 9.03 with CUP 2 or later.	La versione esistente di UCMDB deve essere 9.03 con CUP 2 o versione successiva.
Verifica connessione DB	The host name/IP address validation failed	Il nome host/indirizzo IP del database specificato non è raggiungibile
	The username or password validation failed	Le credenziali utente specificate non sono valide.
	The port validation failed	La porta database specificata non è raggiungibile.
	The SID validation failed	Il SID database specificato non esiste nel DB.
Verifica installazione	The product is already installed	Il prodotto è già installato sull'host di destinazione

Aggiornamento di Configuration Manager

La procedura di aggiornamento verifica automaticamente e convalida quanto segue prima di iniziare:

- la presenza di una connessione funzionante verso il server UCMDB.
- la patch CUP 2 è stata installata per UCMDB.
- la porta JMX è corretta.

Se uno di questi elemento non è stato installato o configurato correttamente, verrà visualizzato un messaggio di errore per informare del problema. È possibile correggere il problema indicato ed eseguire l'aggiornamento.

- Se l'aggiornamento non ha esito positivo perché non è possibile connettersi a UCMDB, verificare che il server UCMDB sia attivo e in esecuzione.
- Se l'aggiornamento non ha esito positivo perché la patch non è stata installata, installare la CUP 2 in relazione alle istruzioni disponibili su: http://support.openview.hp.com/selfsolve/document/FID/DOCUMENTUM_UCMDB_00045
- Se l'aggiornamento ha esito negativo perché la porta JMX di UCMDB non è corretta, selezionare la porta JMX corretta. Per fare ciò, cambiare la proprietà ucmdb.jmx.port nel file **upgrade.properties**, disponibile nella <**directory di installazione di Configuration Manager** >**utilities****Upgrade**\\.

Per eseguire l'aggiornamento, eseguire le seguenti operazioni:

Nota: Verificare che il server UCMDB sia attivo e in esecuzione quando viene iniziata la procedura di aggiornamento.

---

1. Eseguire il backup degli schemi di Configuration Manager e UCMDB.
2. Individuare il file **setup-win64.msi** nella sottocartella Windows del supporto di installazione di Configuration Manager.

3 Fare doppio clic sul file per eseguire la Procedura guidata di installazione di Configuration Manager.

4 Fare clic su **Next** per aprire la pagina Contratto di licenza con l'utente finale.

5 Accettare i termini della licenza e fare clic su **Next** per aprire la pagina Informazioni cliente.

6 Immettere le informazioni e fare clic su **Next** per aprire la pagina Tipo di impostazione.

7 Selezionare la cartella dove verrà installato Configuration Manager. Verificare di aver selezionare una posizione diversa rispetto a quella utilizzata per la versione precedente.

Per impostazione predefinita, Configuration Manager viene installato nella seguente directory: **c:\hp\cnc920**. Fare clic su **Next** per accettare la posizione predefinita, oppure fare clic su **Sfoglia** per selezionare una posizione diversa, quindi fare clic su **Next**.

Nota: la directory di installazione non deve contenere spazi nel nome.

---

8 Fare clic su **Next** per confermare e iniziare l'installazione.

Completata la procedura guidata di installazione, si avvia automaticamente la Procedura di post installazione di Configuration Manager-.

9 Fare clic su **Next** fino a quando viene chiesto di eseguire una nuova installazione di Configuration Manager o di eseguire l'aggiornamento.

10 Selezionare **Aggiorna** e fare clic su **Next**.

11 Completata l'installazione, aprire il file **post_installation.log** (disponibile nella <**directory di installazione di Configuration Manager/tmp/log**) per verificare se l'installazione è stata completata senza errori.

In caso di errori durante l'aggiornamento, viene visualizzato un messaggio che consente di chiudere la procedura guidata. In questo caso contattare l'assistenza HP.

12 Avviare il servizio Configuration Manager.

Nota: dopo l'aggiornamento, è necessario eseguire nuovamente la configurazione SSL. Per informazioni, consultare "Protezione avanzata" a pagina 91.

3

Installazione di HP Universal CMDB Configuration Manager su una piattaforma Linux

Importante: consultare le note sulla versione per le procedure di installazione più aggiornate.

Questo capitolo comprende:

Impostazione di pre installazione

Questa sezione comprende anche:

- "Prerequisiti" a pagina 46
- "Ottenere il file setup.bin" a pagina 46

Prerequisiti

- Almeno 400MB di spazio libero su disco
- Visualizzazione X di lavoro consigliata

Ottenere il file setup.bin

Il file di installazione di Linux (**setup.bin**) si trova nel supporto di installazione o nell'immagine ISO che è possibile scaricare dal sito web HP. Accedere al file in uno dei seguenti modi:

- Montare un DVD su un computer Linux:

```
$ mkdir -p /mnt/cdrom
$ mount /dev/cdrom /mnt/cdrom
```

- Montare un'immagine ISO su un dispositivo a blocchi loopback:

```
$ mkdir -p /mnt/cdrom
$ mount -o loop cnc-<version>.iso /mnt/cdrom
```

- Copiare il file **setup.bin** in una posizione temporanea nel computer Linux.

Installare Configuration Manager

Questa attività descrive come installare Configuration Manager sul server, e come configurare la connessione al database e l'integrazione di UCMDB.

Se si dispone di una visualizzazione X di lavoro, nell'interfaccia utente viene visualizzata la procedura di post installazione; in caso contrario, la procedura di post installazione viene visualizzata in modalità console.

Nota: le procedure descritte nella guida si riferiscono alla modalità console; tuttavia, le stesse procedure vengono visualizzate se si utilizza la procedura guidata interfaccia utente.

Per installare Configuration Manager:

1 Per installare Configuration Manager nella posizione corrente, eseguire il seguente comando:

```
chmod 755 setup.bin
$ /path/to/installation/kit/setup.bin
```

2 Viene visualizzato il Contratto di licenza con l'utente finale (EULA) che deve essere accettato. Scorrere verso il basso dell'EULA facendo clic sulla barra spaziatrice fino a raggiungere la fine dell'EULA. Per accettare e continuare con l'installazione, digitare **sì** e premere **Invio**.

HP Universal CMDB Configuration Manager viene installato nella posizione corrente nella sottocartella **cnc**.

Pagina di benvenuto

```
<=============================>
Welcome
<=============================>
Welcome to the HP Universal CMDB Configuration Manager
post installation wizard.
Enter [<C>ancel] [Ne<x>t]>
```

Premere **Invio** per continuare passando alla pagina successiva.

Selezione del fornitore del database

```
<============================>
Database Connection Configuration
<============================>
-------
Vendor:
-------
  ->1 - Oracle
    2 - Microsoft
Enter index number from 1 to 2 OR [<C>ancel] [Back<b>] [Ne<x>t]>
```

Premere **Invio** per selezionare Oracle, o digitare **2** e premere **Invio** per selezionare Microsoft.

Nome host database

```
-------------
Set Hostname:
-------------
        Hostname: = "localhost"
Input the new Hostname: OR [<C>ancel] [<B>ack] [Ne<x>t]>
```

Immettere il nome host del database e premere **Invio**. Il valore predefinito del nome host è **localhost**.

Porta database

```
---------
Set Port:
---------
        Port: = "1521"
Input the new Port: OR [<C>ancel] [<B>ack] [Ne<x>t]>
```

La porta predefinita per Oracle è 1521, mentre la porta pedefinita per Microsoft è 1433. Per utilizzare un numero diverso di porta, inserire il numero e premere **Invio**.

Nome SID/DB

```
-----------
Set SID/DB:
-----------
        SID/DB: = "orcl"
Input the new SID/DB: OR [<C>ancel] [<B>ack] [Ne<x>t]>
```

Per Oracle, questo campo specifica il SID del database; per Microsoft, questo campo specifica il nome del database. Immettere un valore valido e premere **Invio**.

Nome utente/schema e password

```
-------------
Set Username:
-------------
Input the Username: OR [<C>ancel] [<B>ack] [Ne<x>t]>
```

Immettere il nome utente del database e premere **Invio**.

```
Input the Password: OR [<C>ancel] [<B>ack] [Ne<x>t]>
```

Immettere la password dello schema e premere **Invio**.

Test connessione database

```
--------
Set Test
--------
        Test = "Yes"
Choose [<Y>es]/[<N>o] for Test OR [<C>ancel] [<B>ack] [Ne<x>t]>
```

Premere **Invio** per testare la connessione al database.

Poiché la procedura guidata tenta di creare le tabelle nello schema database, si consiglia di testare la connessione al database. Per non eseguire il test della connessione, immettere **No** e premere **Invio**.

Una volta completato con successo il test della connessione al database, viene visualizzato il seguente messaggio:

```
success
Enter [<C>ancel] [<B>ack] [Ne<x>t]>
```

Premere **Invio** per continuare. In caso di errori nel test della connessione, viene visualizzato un messaggio di errore dove viene chiesto di eseguire nuovamente il test. Correggere il problema di connessione, eseguire nuovamente il test e continuare l'installazione.

Nome host server applicazioni

```
<=============================>
Application Server Configuration
<=============================>
Hostname:
----
Set
----
         = "myucmdbcmhost.mydomain"
Input the new  OR [<C>ancel] [Back<b>] [Ne<x>t]>
```

Il valore predefinito per il nome host è il nome host effettivo del computer. Se si sta eseguendo l'installazione dopo il bilanciamento di carico o un proxy server, immettere qui il nome esterno.

Personalizzazione delle porte server applicazione

```
-------------------
Select Customize ports
-------------------
        Customize ports = "No"
Choose [<Y>es]/[<N>o] for Customize ports OR [<C>ancel] [<B>ack]
[Ne<x>t]>
```

Per utilizzare le porte predefinite per Configuration Manager, premere **Invio**. Per utilizzare le porte personalizzate, immettere **Yes** e premere **Invio**. I numeri di porta predefiniti sono:

Nome porta	Numero porta
HTTP	8180
HTTPS	8443
Gestione Tomcat	8005
AJP	8009
HTTP JMX	39900
RMI JMX	39600

Se si sceglie di personalizzare le porte, per ciascuna delle porte elencate in precedenza verrà chiesto di specificare un valore. Immettere il nuovo valore e premere **Invio** per ciascuna:

```
HTTP port:
----
Set
----
         = "8180"
Input the new  OR [<C>ancel] [<B>ack] [Ne<x>t]>
HTTPS port:
----
Set
----
         = "8443"
Input the new  OR [<C>ancel] [<B>ack] [Ne<x>t]>
Tomcat port:
----
Set
----
         = "8005"
Input the new  OR [<C>ancel] [<B>ack] [Ne<x>t]>
AJP port:
----
Set
----
         = "8009"
Input the new  OR [<C>ancel] [<B>ack] [Ne<x>t]>
JMX HTTP port:
----
Set
----
         = "39900"
Input the new  OR [<C>ancel] [<B>ack] [Ne<x>t]>
JMX remote port:
----
Set
----
         = "39600"
Input the new  OR [<C>ancel] [<B>ack] [Ne<x>t]>
```

Utente amministrativo iniziale

```
<============================>
Users Credentials
<============================>
Initial Administrative User
Admin username:
----
Set
----
Input the  OR [<C>ancel] [Back<b>] [Ne<x>t]>
```

Un utente amministrativo iniziale viene creato per essere amministratore o super-utente del sistema per l'accesso iniziale. Immettere il nome utente dell'amministratore da utilizzare, quindi premere **Invio**.

```
Admin password:
Input the  OR [<C>ancel] [<B>ack] [Ne<x>t]>
```

Immettere la password per l'utente amministratore e premere **Invio**.

```
Confirm password:
Input the  OR [<C>ancel] [<B>ack] [Ne<x>t]>
```

Per conferma, immettere nuovamente la password per l'utente amministratore e premere **Invio**.

Utente di integrazione

```
Platform Integration User
Integration username:
----
Set
----
Input the  OR [<C>ancel] [<B>ack] [Ne<x>t]>
```

Selezionare il nome utente di integrazione di UCMDB. Questo utente viene creato in UCMDB durante il processo di post installazione. HP consiglia di utilizzare il nome utente che renda chiaro il suo scopo per l'integrazione (ad esempio, cm_integration). Immettere il nome utente selezionato e premere **Invio**.

```
Integration password:
Input the  OR [<C>ancel] [<B>ack] [Ne<x>t]>
```

Immettere la password per l'utente di integrazione e premere **Invio**.

```
Confirm password:
Input the  OR [<C>ancel] [<B>ack] [Ne<x>t]>
```

Per conferma, immettere nuovamente la password per l'utente di integrazione e premere **Invio**.

Nome host server HP Universal CMDB

```
<============================>
HP UCMDB Connection Configuration
<============================>
Hostname:
----
Set
----
         = "localhost"
Input the new  OR [<C>ancel] [Back<b>] [Ne<x>t]>
```

Immettere il nome host per il server UCMDB e premere **Invio**. Probabilmente sarà diverso dal localhost predefinito, pertanto si consiglia di non installare UCMDB e Configuration Manager sullo stesso computer nell'ambiente di produzione.

Porta server HP Universal CMDB

```
Port:
----
Set
----
         = "8080"
Input the new  OR [<C>ancel] [<B>ack] [Ne<x>t]>
```

Premere **Invio** per accettare il numero di porta predefinito 8080 per il server UCMDB, oppure immettere un numero di porta e premere **Invio**.

Protocollo server HP Universal CMDB

```
Protocol:
  ->1 - HTTP
    2 - HTTPS
Enter index number from 1 to 2 OR [<C>ancel] [<B>ack] [Ne<x>t]>
```

Premere **Invio** per usare HTTP, oppure immettere 2 e premere **Invio** per usare HTTPS.

Nota: selezionando HTTPS sarà necessario scambiare le chiavi con UCMDB. Per informazioni, consultare "Protezione avanzata" a pagina 91. Questa procedura imposta HTTPS con un certificato autofirmato non protetto.

Cliente server HP Universal CMDB

```
Customer:
----
Set
----
         = "Default Client"
Input the new  OR [<C>ancel] [<B>ack] [Ne<x>t]>
```

Premere **Invio** per accettare il numero cliente predefinito per il server UCMDB, oppure immettere un nome cliente e premere **Invio**.

Credenziali Sysadmin server HP Universal CMDB

```
Administrative username:
----
Set
----
Input the  OR [<C>ancel] [<B>ack] [Ne<x>t]>
```

Immettere il nome utente sysadmin del server UCMDB. È l'utente che può eseguire i metodi JMX sul server UCMDB. È un utente pre esistente e non viene creato durante l'installazione. Ottenere le credenziali per l'utente sysadmin dall'amministratore del server UCMDB.

```
Administrative password:
Input the  OR [<C>ancel] [<B>ack] [Ne<x>t]>
```

Immettere la password per l'utente sysadmin del server UCMDB e premere **Invio**.

Connessione server HP Universal CMDB

```
--------
Set Test
--------
        Test = "Yes"
Choose [<Y>es]/[<N>o] for Test OR [<C>ancel] [<B>ack] [Ne<x>t]>
```

Premere **Invio** per testare la connessione al server UCMDB. Poiché la procedura guidata tenta di distribuire i pacchetti e configurare il server UCMDB, si consiglia di testare la connessione con il server. Per non eseguire il test della connessione, immettere **No** e premere **Invio**.

Una volta completato con successo il test della connessione con il server, viene visualizzato il seguente messaggio:

```
success
Enter [<C>ancel] [<B>ack] [Ne<x>t]>
```

Premere **Invio** per continuare. In caso di errori nel test della connessione, viene visualizzato un messaggio di errore dove viene chiesto di eseguire nuovamente il test. Correggere il problema di connessione, eseguire nuovamente il test e continuare l'installazione.

Riepilogo

La procedura guidata visualizza un riepilogo di tutte le scelte fatte prima di eseguirle effettivamente:

```
<===========================>
Post Installation Actions Summary
<===========================>
Post installation actions summary
Users
-----
HP Universal CMDB Configuration Management admin username: admin
HP Universal CMDB Platform integration username: cm_integration

Database
--------
Vendor: Oracle
Host: mydbhost.mydomain
Port: 1521
SID/DB: orcl
Encrypt password? Yes
Create schema objects? Yes

Application Server
------------------
hostname: myucmdbcmhost.mydomain
HTTP: 8180
HTTPS: 8443
Tomcat management: 8005
AJP: 8009
JMX HTTP: 39900
JMX remote: 39600
Debug: 7878

Windows Service
---------------
Create service? No

HP Universal CMDB Platform
-----
URL: http://myucmdb.mydomain:8080
Sysadmin username: sysadmin
Customer: Default Client

Enter [<C>ancel] [Back<b>] [Ne<x>t]>
```

Premere **Invio** per continuare con la fase di configurazione. Durante il processo di configurazione viene visualizzata una barra di avanzamento. La procedura guidata esegue le seguenti attività:

1. Crea le tabelle e gli oggetti del database.
2. Popola il database con i valori predefiniti e iniziali.
3. Crea l'utente amministrativo iniziale.
4. Crea l'utente di integrazione nel server UCMDB.
5. Consolida il server UCMDB.
6. Crea lo stato autorizzato nel server UCMDB.
7. Distribuisce i pacchetti di Configuration Manager sul server UCMDB.

Una volta completata la configurazione, viene visualizzato il seguente messaggio:

```
<============================>
Finish
<============================>
Post installation configuration has completed.
Enter [Finish<f>]>
```

Premere **Invio** per uscire dalla procedura guidata.

Opzioni di installazione in batch

È possibile installare Configuration Manager in modalità batch. In questo modo vengono estratti solamente i file dal pacchetto di installazione, ma non esegue alcuna configurazione di post installazione. Per eseguire l'installazione in modalità batch, eseguire il seguente comando:

```
$ /path/to/installation/kit/setup.bin –silent
```

Eseguire il server applicazioni di Configuration Manager

Per eseguire Configuration Manager, eseguire i seguenti comandi:

```
$ cd /path/to/installation/location
$ ./start-server-0.sh
```

È possibile creare uno script nella directory **/etc/init.d** per avviare automaticamente Configuration Manager all'avvio del computer.

4

Accedere a Configuration Manager

Questo capitolo comprende:

Accesso a Configuration Manager

L'accesso a Configuration Manager viene effettuato utilizzando un browser Web da qualunque computer dotato di una connessione di rete (Intranet o Internet) al server di Configuration Manager. Il livello di accesso concesso a un utente dipende dalle autorizzazioni dell'utente. Per informazioni sulla concessione delle autorizzazioni dell'utente, consultare "Gestione utenti" nella Guida dell'utente di *HP Universal CMDB Configuration Manager*.

Per informazioni sui requisiti del browser Web, così come i requisiti minimi per la visualizzazione di Configuration Manager, consultare "Matrice di supporto" a pagina 16.

Per informazioni sull'accesso protetto a Configuration Manager, consultare "Protezione avanzata" a pagina 91.

Per informazioni sulla risoluzione dei problemi relativi all'accesso a Configuration Manager, consultare "Risoluzione dei problemi" a pagina 127.

Accedere a Configuration Manager

1. Nel browser Web, immettere l'URL del server Configuration Manager, ad esempio, http://<nome server o indirizzo IP>.<nome dominio>:<porta>/cnc, dove **<nome server o indirizzo IP>.<nome dominio>** rappresentano il nome dominio completo (FQDN) del server Configuration Manager, mentre la **<porta>** rappresenta la porta selezionata durante l'installazione.
2. Immettere il nome utente e la password definiti nella Procedura guidata post installazione di Configuration Manager.
3. Fare clic su **Accesso**. Una volta eseguito l'accesso, il nome utente viene visualizzato nella parte superiore destra dello schermo.
4. (Consigliato) Effettuare la connessione al server LDAP organizativo e assegnare i ruoli amministrativi agli utenti LDAP per consentire agli amministratori di Configuration Manager di accedere al sistema. Per informazioni su come assegnare i ruoi agli utenti nel sistema Configuration Manager, cosultare "Gestione utenti" nella Guida dell'utente di *HP Universal CMDB Configuration Manager*.

Disconnessione

Una volta completata la sessione, si consiglia di disconnettersi dal sito Web per evitare accessi non autorizzati.

Per disconnettere, fare clic su **Disconnetti** nella parte superiore della pagina.

Nota: la scadenza predefinita per la sessione è di 30 minuti.

Accesso alla console JMX per Configuration Manager

Per ambiti relativi alla risoluzione dei problemi o per modificare alcune configurazioni, potrebbe essere necessario accedere alla console JMX.

Per accedere alla console JMX:

1 Aprire la console JMX su http://<nome server o indirizzo IP>:<porta>/cnc/jmx-console. La porta è quella configurata durante l'installazione di Configuration Manager.

2 Immettere le credenziali utente predefinite. Sono le stesse credenziali utente utilizzate per l'accesso a Configuration Manager.

5

Altri casi di utilizzo

Questo capitolo comprende:

Trasferire l'installazione di Configuration Manager tra i computer

Questa procedura deve essere utilizzata quando si desidera trasferire una installazione di Configuration Manager da un computer ad un altro conservando lo schema database intatto e il collegamento con lo stesso server UCMDB.

1. Nella <**directory di installazione di Configuration Manager** >**\cnc\bin**, eseguire il seguente comando: edit-server-0.bat.
2. Registrare tutti i parametri trovati, comprese le porte (ad esempio la porta JMX).
3. Interrompere l'esecuzione del server Configuration Manager sul computer di origine. (Se sul computer è installato un sistema Windows, procedere interrompendo l'esecuzione del servizio Configuration Manager).

4 Installare Configuration Manager sul computer di destinazione:

➤ Su Windows: eseguire il file **setup-win64.msi** (disponibile nella cartella **windows** del supporto di installazione).

➤ Su Linux: seguire le istruzioni in "Installare Configuration Manager" a pagina 47.

5 Annullare la Procedura di post installazione quando inizia.

6 Copiare tutti i file dalla directory di installazione precedente sul computer di origine nella posizione della nuova installazione sul computer di destinazione.

7 Nel computer di destinazione, sostituire il nome host con il nome del computer di destinazione in **client-config.properties** e **resources.properties** (disponibili nella cartella **conf**).

Nota: se il computer di destinazione si trova in un dominio diverso dal computer di origine, modificare anche il dominio di riferimento precedente nel file **lwssofmconf.xml**.

---

8 Nel computer di destinazione, eseguire il file **bin/create-windows-service.bat** per creare il servizio Windows. Impostare il contrassegno **-h** per visualizzare le opzioni disponibili ed utilizzare i parametri registrati dal servizio del computer di origine (registrati nel passaggio 2) come necessario. Per il parametro nome dominio, utilizzare server-0. Utilizzando i valori predefiniti, il comando avrà il seguente aspetto:

c:\HP\cnc920\bin>create-windows-service.bat -j 39900 -n server-0 -r 39600

9 Avviare l'esecuzione del server Configuration Manager sul computer di destinazione.

Cambiare i numeri di porta dopo l'installazione

1 Interrompere l'esecuzione del server Configuration Manager.

2 Eseguire il backup dei contenuti della <**directory di installazione di Configuration Manager**>**servers****server-0**.

3 Eliminare la <**directory di installazione di Configuration Manager**>**servers**\\
server-0.

4 Eseguire lo script **create-node.bat** con il contrassegno **-h** per visualizzare le opzioni disponibili. Passare tutti i numeri di porta necessari all'utilità.

5 Nel computer di destinazione, sostituire la porta con il nuovo numero di porta HTTP in **client-config.properties** e **resources.properties** (disponibili nella cartella **conf**).

6 Eseguire lo script **edit-server-0.bat**, disponibile nella <**directory di installazione di Configuration Manager**>**bin**.

7 (Per i sistemi Windows) Nella finestra Proprietà di HP Universal CMDB Configuration Manager che si apre, fare clic sulla scheda Java e cambiare le impostazioni **jmx.http.port** e **com.sun.management.jmxremote.port** sui nuovi numeri di porta.

8 Avviare l'esecuzione del servizio Configuration Manager sul computer di destinazione.

Copiare le impostazioni di sistema tra i sistemi



1 Sul computer di origine, aprire Configuration Manager. Passare a **Sistema** > **Impostazioni** e fare clic sul pulsante **Esporta set di configurazione in un file zip**.

   Prima di eseguire l'esportazione, è possibile escludere delle parti specifiche della configurazione deselezionare la casella di controllo accanto agli elementi della configurazione attinenti.

2 Copiare la configurazione esportata sul computer di destinazione.



3 Sul computer di destinazione, aprire Configuration Manager. Passare a **Sistema** > **Impostazioni** e fare clic sul pulsante **Importa set di configurazione**.

Backup e ripristino

È possibile eseguire il backup di una installazione di Configuration Manager in modo da poter eseguire il ripristino da un qualsiasi tipo di errore che altrimenti richiederebbe una nuova installazione completa.

Backup

Eseguire il backup delle seguenti informazioni:

➤ le sottocartelle **conf** e **security** nella directory di installazione di Configuration Manager. Questa procedura può essere eseguire mentre il sistema è attivo e in esecuzione, senza dover interrompere il funzionamento.

➤ lo schema del database

Ripristino (su un sistema Windows)

Questa procedura deve essere eseguita su un nuovo sistema che ancora non ha Configuration Manager installato.

1. Installare Configuration Manager sul computer di destinazione eseguendo il file **setup-win64.msi** (disponibile nella cartella **windows** del supporto di installazione) modalità batch come segue:

   ```
   msiexec /i setup-win64.msi TARGETDIR=path\to\install\dir /passive
   ```

2. Ripristinare le directory **conf** e **security**. Utilizzare il metodo di ripristino corrispondente a quello utilizzato per il backup. Sovrascrivere le directory create con l'installazione eseguita nel passaggio 1.
3. Ripristinare lo schema del database. Se si esegue il ripristino su un server database diverso, è necessario modificare la proprietà **url** nel file **database.properties** (disponibile nella directory **conf**) in modo che corrisponda al nuovo nome server database.
4. Utilizzare l'utilità **create-windows-service** (con il contrassegno **-h** per visualizzare le opzioni disponibili) per creare un servizio Windows.
5. Avviare il server Configuration Manager.

Ripristino (su un sistema Linux)

1. Installare Configuration Manager sul computer di destinazione eseguendo il file **setup.bin** (disponibile nel supporto di installazione). Per informazioni, consultare "Installare Configuration Manager" a pagina 47, ma annullare l'installazione al primo passaggio della procedura di post-installazione. Tutti i file saranno distribuiti anche se il sistema non sarà configurato.
2. Ripristinare le directory **conf** e **security**. Utilizzare il metodo di ripristino corrispondente a quello utilizzato per il backup. Sovrascrivere quelle create con l'installazione eseguita nel passaggio 1.
3. Ripristinare lo schema del database. Se si esegue il ripristino su un server database diverso, è necessario modificare la proprietà **url** nel file **database.properties** (disponibile nella directory **conf**) in modo che corrisponda al nuovo nome server database.
4. Avviare il server Configuration Manager.

6

Configurazione avanzata

Questo capitolo comprende:

Opzioni avanzate di connessione al database

Nel caso siano necessarie proprietà avanzate di connessione al database per supportare la distribuzione del database, è possibile procedere una volta completata l'esecuzione della Procedura guidata di post installazione. Configuration Manager supporta tutte le opzioni di connessione al database supportate dal driver JDBC del fornitore e possono essere configurate utilizzando l'URL di connessione al database. Per configurare altre connessioni avanzate, modificare la proprietà **jdbc.url** nel file <**Configuration Manager installation directory**>**conf****database.properties**.

Nota: Procedere come segue quando si esegue la configurazione avanzata su un sistema Linux:

- Cambiare la direzione delle barre oblique nelle istruzioni per le barre (/).
- Sostituire **.bat** con **.sh** nelle esecuzioni script.

I seguenti esempi illustrano le opzioni avanzate per Microsoft SQL Server:

- **Autenticazione Windows (NTLM).** Per applicare l'autenticazione Windows, aggiungere la proprietà del dominio all'URL di connessione JTDS nel file database.properties. Specificare il dominio Windows per l'autenticazione.

  Ad esempio:

  ```
  jdbc:jtds:sqlserver://myServer:1433/myDatabase;sendStringParametersAsUnicode
  =false;domain=myDomain
  ```

- **SSL.** Per informazioni sulla protezione della connessione del server MS SQL utilizzando SSL, consultare http://jtds.sourceforge.net/faq.html.

I seguenti esempi illustrano le opzioni avanzate per Oracle Database Server:

- **URL Oracle.** Specificare l'URL di connessione del driver nativo di Oracle. Specificare un nome server e un SID Oracle validi. Se si utilizza **Oracle RAC**, specificare in alternativa i dati di configurazione di Oracle RAC.

  Nota: per ulteriori informazioni sul formato URL del driver JDBC nativo di Oracle, consultare http://www.orafaq.com/wiki/JDBC#Thin_driver. Per ulteriori informazioni sulla configurazione dell'URL per Oracle RAC, consultare
  http://download.oracle.com/docs/cd/B28359_01/java.111/e10788/rac.htm.

- **SSL.** Per informazioni sulla protezione della connessione a Oracle utilizzando SSL, consultare le spiegazioni di seguito:
  - http://download.oracle.com/docs/cd/E11882_01/network.112/e10746/asojbdc.htm#ASOAG9604
  - http://download.oracle.com/docs/cd/E11882_01/java.112/e16548/clntsec.htm#insertedID6

Configurazione database - Supporto MLU (Multi-Lingual Unit)

Questa sezione descrive le impostazioni del database necessario per la localizzazione del supporto.

Impostazioni Oracle Server

La tabella di seguito elenca le impostazioni necessarie per Oracle Server:

Opzione	Supportato	Consigliato	Note
Set di caratteri	WE8ISO8859P1; UTF8,AL32UTF8	AL32UTF8	

Impostazioni Microsoft SQL Server

La tabella di seguito elenca le impostazioni necessarie per Microsoft SQL Server:

<table>
<tr><th>Opzione</th><th>Supportato</th><th>Consigliato</th><th>Note</th></tr>
<tr><td>Raccolta</td><td>Maiuscole/Minuscole. HP Universal CMDB Non supporta l'ordinamento binario e la distinzione tra maiuscole e minuscole. L'ordinamento con distinzione tra maiuscole e minuscole è supportato solo con una combinazione di accenti, kana o impostazioni di larghezza.</td><td>Utilizza la finestra di dialogo Impostazioni raccolta per selezionare la raccolta. Non selezionare la casella di controllo binario. Accento, kana e distinzione larghezza devono essere selezionati in base ai requisiti per la lingua dati attinenti. La lingua selezionata deve essere la stessa delle impostazioni internazionali del sistema operativo Windows.</td><td rowspan="2">Si limita alla Raccolta locale e alle definizioni inglesi predefinite.</td></tr>
<tr><td>Raccolta proprietà database</td><td colspan="2">Predefinito del server</td></tr>
</table>

Nota:

Per tutte le lingue: **<Lingua>_CI_AS** è l'opzione minima richiesta.
Ad esempio, in Giapponese, se si desidera selezionare le opzioni Distinzione Kana e Distinzione larghezza, l'opzione consigliata è:
Japanese_CI_AS_KS_WS o **Japanese_90_CI_AS_KS_WS**. Questo consiglio indica che i caratteri giaponesi sono di tipo Distinzione accento, Distinzione Kana e Distinzione larghezza.

- **Distinzione accento (_AS).** Distingue tra i caratteri accentati e non accentati. Ad esempio, **a** non è uguale a **á**. Se l'opzione non è selezionata, Microsoft SQL Server considera identiche le versioni accentate e non accentate delle lettere per scopi di ordinamento.
- **Distinzione Kana (_KS).** Distingue tra i due tipi di caratteri kana giapponesi: Hiragana e Katakana. Se l'opzione non è selezionata, Microsoft SQL Server considera i caratteri Hiragana e Katakana uguali per scopi di ordinamento.
- **Distinzione larghezza (_WS).** Distingue tra caratteri a byte singolo e caratteri uguali quando rappresentati come caratteri a byte doppio. Se l'opzione non è selezionata, Microsoft SQL Server considera identica la rappresentazione a byte singolo e a byte doppio dello stesso carattere per scopi di ordinamento.

Single Sign-On (SSO)

Il Single sign-on tra Configuration Manager e UCMDB viene eseguito utilizzando la tecnologia LWSSO di HP. Per informazioni, consultare "Autenticazione Lightweight Single Sign-On (LW-SSO) – Riferimenti generali" a pagina 121.

Questa sezione comprende:

Abilitare LW-SSO tra Configuration Manager e UCMDB

Alcuni utenti di Configuration Manager dispongono anche dell'autorizzazione di accesso a UCMDB. Per facilità d'uso, Configuration Manager offre un collegamento diretto all'interfaccia utente di UCMDB (selezionare **Amministrazione** > **UCMDB Foundation**). Per utilizzare single sign-on (che preclude la necessità di accedere a UCMDB una volta eseguito l'accesso a Configuration Manager), è necessario abilitare LW-SSO sia per Configuration Manager che UCMDB e assicurarsi che entrambi lavorino con lo stesso initString. Questa attività deve essere eseguita manualmente a meno che non sia stata già eseguita come parte dell'installazione di Deployment Manager.

Per abilitare LW-SSO:

1 Nella directory di installazione di Configuration Manager, modificare il file **\conf\lwssofmconf.xml**.

2 Individuare la sezione seguente:

```
enableLWSSO enableLWSSOFramework="true"
```

e verificare che il valore sia **true**.

3 Individuare la sezione seguente:

```
lwssoValidation  id="ID000001">
<domain> </domain>
```

e immettere il dominio del server Configuration Manager dopo <**domain**>.

4 Individuare la sezione seguente:

```
<initString="Questa stringa deve essere sostituita"></crypto>
```

e sostituire "Questa stringa deve essere sostituita" con una stringa condivisa utilizzata da tutte le applicazioni considerate attendibili che interagiscono con LW-SSO.

5 Individuare la sezione seguente:

```
<!--multiDomain>
<trustedHosts>
<DNSDomain>Questo valore deve essere sostituito dal domino
dell'applicazione</DNSDomain>
<DNSDomain>Questo valore deve essere sostituito dal domino dell'altra
applicazione</DNSDomain>
</trustedHosts>
</multiDomain-->
```

Nota: il secondo DNSDomain deve essere incluso solo se Configuration Manager e un'altra applicazione sono situate su domini diversi.

Rimuovere il delimitatore all'inizio e immettere tutti i domini del server (se necessario) negli elementi DNSDomain (al posto di Questo valore deve essere sostituito dal domino dell'applicazione o Questo valore deve essere sostituito dal domino dell'altra applicazione. L'elenco deve includere il dominio del server immesso nel passaggio 3 a pagina 76.

6 Salvare il file con i cambiamenti e riavviare il server.

7 Avviare il browser Web e specificare il seguente indirizzo: http://<UCMDB server address>.<domain_name>:8080/jmx-console.

Immettere le credenziali di autenticazione della console JMX, che per impostazione predefinita sono:

- Nome di accesso = **sysadmin**
- Password = **sysadmin**

8 In **UCMDB-UI**, selezionare **Configurazione LW-SSO** per aprire la pagina JMX MBEAN View.

9 Selezionare il metodo **setEnabledForUI**, impostare il valore su **true** e fare clic su **Invoke**.

10 Selezionare il metodo **setDomain**. Immettere il nome del dominio del server UCMDB e fare clic su **Invoke**.

11 Selezionare il metodo **setInitString**. Immettere lo stesso initString immesso per Configuration Manager nel passaggio 4 a pagina 77 e fare clic su **Invoke**.

12 Se Configuration Manager e UCMDB sono posizionati nello stesso dominio, selezionare il metodo **addTrustedDomains** e immettere i nomi dei domini dei server UCMDB e Configuration Manager. Fare clic su **Invoke**.

13 Per visualizzare la configurazione LW-SSO come è stata salvata nel meccanismo impostazioni, selezionare il metodo **retrieveConfigurationFromSettings** e fare clic su**Invoke**.

14 Per visualizzare la configurazione LW-SSO effettiva caricata, selezionare il metodo **retrieveConfiguration** e fare clic su **Invoke**.

Configurare LW-SSO in Operations Orchestration

Se LW-SSO è abilitato sia su Configuration Manager che Operations Orchestration (OO), gli utenti che hanno eseguito l'accesso a Configuration Manager possono accedere a Operations Orchestration a livello web senza dover specificare il nome utente e la password (per gli amministratori di sistema).

Nota:

- Nella procedura seguente, <OO_HOME> rappresenta la home directory di Operations Orchestration.
- LW-SSO richiede che gli account utilizzati per accedere a Operations Orchestration e Configuration Manager abbiamo lo stesso nome account (ma con password diverse).
- LW-SSO richiede che l'account in Operations Orchestration non sia interno.

Per configurare LW-SSO in Operations Orchestration:

1. Arrestare il servizio RSCentral.
2. In <**OO_HOME**>**Central****WEB-INF****applicationContext.xml**, abilitare l'importazione tra LWSSO_SECTION_BEGIN e LWSSO_SECTION_END come indicato di seguito:

```
<!-- LWSSO_SECTION_BEGIN-->
        <import resource="CentralLWSSOBeans.xml"/>
<!--LWSSO_SECTION_END -->
```

3. In <**OO_HOME**>**Central****WEB-INF****web.xml**, abilitare tutti i filtri e le mappature tra LWSSO_SECTION_BEGIN e LWSSO_SECTION_END come indicato di seguito:

```
<!-- LWSSO_SECTION_BEGIN-->

<filter>
        <filter-name>LWSSO</filter-name>
        <filter-
    class>com.iconclude.dharma.commons.util.http.DharmaFilterToBeanProx
    y
```

```
            </filter-class>
            <init-param>
                <param-name>targetBean</param-name>
                <param-value>dharma.LWSSOFilter</param-value>
            </init-param>
    ......
    </filter>
<!--LWSSO_SECTION_END -->

<!-- LWSSO_SECTION_BEGIN-->
    <filter-mapping>
        <filter-name>LWSSO</filter-name><url-pattern>/*</url-pattern>
    </filter-mapping>
<!--LWSSO_SECTION_END -->

<!-- LWSSO_SECTION_BEGIN-->
    <filter-mapping>
        <filter-name>LWSSO2Acegi</filter-name><url-pattern>/*</url-pattern>
    </filter-mapping>
    <filter-mapping>
        <filter-name>dharmaLWSSOGroupsFilter</filter-name><url-
    pattern>/*</url-pattern>
        </filter-mapping>
<!--LWSSO_SECTION_END -->
```

4 In <**OO_HOME**>**Central****conf****lwssofmconf.xml**, modificare i seguenti due parametri:

- domain: nome dominio del server OO.
- initString: deve essere lo stesso valore initString presente nella configurazione di OO LW-SSO (lunghezza minima: 12 caratteri). Ad esempio, smintegrationlwsso.

Ad esempio:

```
<webui>
<validation>
        <in-ui-lwsso>
         <lwssoValidation  id="ID000001">
                <domain>asia.hpqc.net</domain>
                <crypto cipherType="symmetricBlockCipher"
                                        engineName="AES" paddingModeName="CBC"
keySize="256"  encodingMode="Base64Url"
                                        initString=" smintlwsso "></crypto>
         </lwssoValidation>
        </in-ui-lwsso>
</validation>
<creation>
         <lwssoCreationRef id="ID000002">
                <lwssoValidationRef refid="ID000001"/>
                <expirationPeriod>600000</expirationPeriod>
         </lwssoCreationRef>
</creation>
</webui>
```

5 Riavviare il servizio RSCentral per rendere effettiva la configurazione.

Eseguire l'autenticazione gestione identità

Questa attività descrive come configurare HP Universal CMDB Configuration Manager per accettare l'Autenticazione gestione attività.

Se si utilizza Gestione identità e si decide di aggiungere HP Universal CMDB Configuration Manager, è necessario svolgere questa attività.

Questa attività include le seguenti fasi:

- "Prerequisiti" a pagina 81
- "Configurare HP Universal CMDB Configuration Manager per accettare la gestione identità" a pagina 82

Prerequisiti

Il server Configuration Manager Tomcat deve essere collegato al proprio server Web (IIS o Apache) protetto tramite Gestione identità tramite un connettore Tomcat Java (AJP13).

Per le istruzioni sull'utilizzo di un connettore Tomcat Java (AJP13), consultare la documentazione di Tomcat Java (AJP13).

Configurare HP Universal CMDB Configuration Manager per accettare la gestione identità

Per configurare Tomcat Java (AJP13) con IIS6:

1 Configurare Gestione identità per inviare una intestazione/richiamata di personalizzazione che contiene il nome utente e richiedere il nome dell'intestazione.

2 Aprire la <**directory di installazione di Configuration Manager**>**conf****lwssofmconf.xml** e individuare la sezione che inizia con **in-ui-identity-management**.

Ad esempio:

```
<in-ui-identity-management enabled="false">
  <identity-management>
 <userNameHeaderName>sm-user</userNameHeaderName>
  </identity-management>
</in-ui-identity-management>
```

a Attivare la funzionalità rimuovendo il delimitatore.

b Sostituire **enabled**="**false**" con **enabled**="**true**".

c Sostituire **sm-user** con il nome intestazione richiesto nella fase 1.

3 Aprire il file <**directory di installazione di Configuration Manager**>**conf****client-config.properties** e modificare le seguenti proprietà:

a Cambiare **bsf.server.url** nella URL Gestione identità e la porta nella porta Gestione identità:

bsf.server.url=http://< Identity Manager URL>:< Identity Manager port >/bsf

b Cambiare **bsf.server.services.url** nel protocollo HTTP e la porta nella porta Configuration Manager originale:

bsf.server.services.url=http://<Configuration Manager URL>:
<Configuration Manager Port>/bsf

Esempio di utilizzo di Java Connector per configurare la Gestione identità per Configuration Manager con IIS6 su un sistema operativo Windows 2003

Questa attività di esempio descrive come installare e configurare Java Connector in modo da utilizzarlo per configurare la Gestione identità da utilizzare con Configuration Manager con IIS6 in esecuzione su sistema operativo Windows 2003.

Per installare Java Connector e configurarlo per IIS6 su Windows 2003:

1. Scaricare la versione più recente di Java Connector (ad esempio, **djk-1.2.21**) dal sito Web Apache.
   - **a** Fare clic su http://www.apache.org/dist/tomcat/tomcat-connectors/jk/binaries
/win64/.
   - **b** Selezionare la versione più recente.
   - **c** Scaricare il file **isapi_redirect.dll** dalla directory **amd64**.
2. Salvare il file nella **<directory di installazione di Configuration Manager>\tomcat\bin\win32**.
3. Creare un nuovo file di testo con il nome **isapi_redirect.properties** nella stessa directory con isapi_redirect.dll.

   Il contenuto del file è:

```
# Configuration file for the Jakarta ISAPI Redirector
# The path to the ISAPI Redirector Extension, relative to the website
# This must be in a virtual directory with execute privileges
extension_uri=/jakarta/isapi_redirect.dll
# Full path to the log file for the ISAPI Redirector
log_file=<Configuration Manager installation directory>\servers
\server-0\logs\isapi.log
# Log level (debug, info, warn, error or trace)
log_level=info
# Full path to the workers.properties file
worker_file==<Configuration Manager installation directory>\tomcat
\conf\workers.properties.minimal
# Full path to the uriworkermap.properties file
worker_mount_file==<Configuration Manager installation directory>\tomcat
\conf\uriworkermap.properties
```

4 Creare un nuovo file di testo con il nome **workers.properties.minimal** nella <**directory di installazione diConfiguration Manager**>**\tomcat\conf**.

Il contenuto del file è:

```
# workers.properties.minimal -
#
# This file provides minimal jk configuration
# properties needed to
# connect to Tomcat.
#
# Defining a worker named ajp13w and of type ajp13
# Note that the name and the type do not have to
# match.
        worker.list=ajp13w
        worker.ajp13w.type=ajp13
        worker.ajp13w.host=localhost
        worker.ajp13w.port=8009
#END
```

5 Creare un nuovo file di testo con il nome **uriworkermap.properties** nella <**directory di installazione diConfiguration Manager**>**\tomcat\conf**.

Il contenuto del file è:

```
# uriworkermap.properties - IIS
#
# This file provides sample mappings for example:
# ajp13w worker defined in workermap.properties.minimal
# The general syntax for this file is:
# [URL]=[Worker name]
/cnc=ajp13w
/cnc/*=ajp13w
/bsf=ajp13w
/bsf/*=ajp13w
#END
```

Importante: si noti che Configuration Manager deve avere due regole. La nuova sintassi consente di riunirle in una sola regola, ad esempio:

/cnc|/*=ajp13w

---

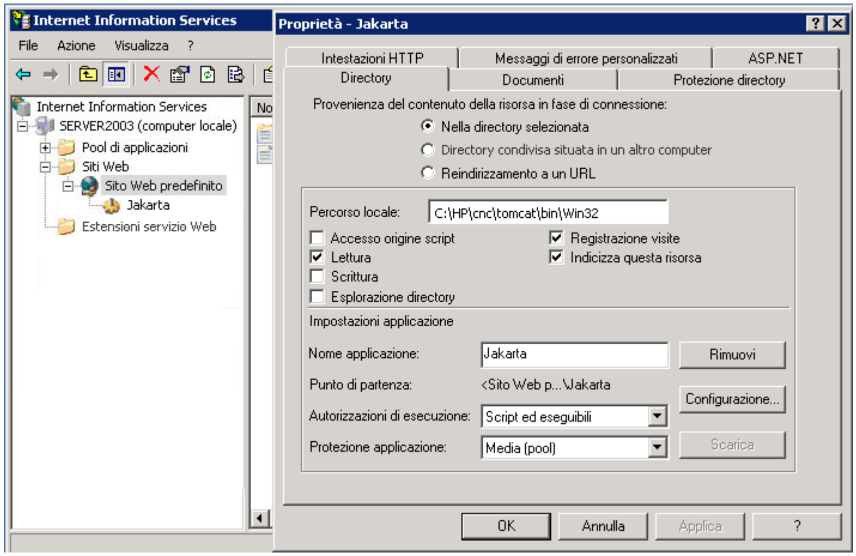
6 Creare la directory virtuale nell'oggetto sito Web corrispondente nella configurazione IIS.

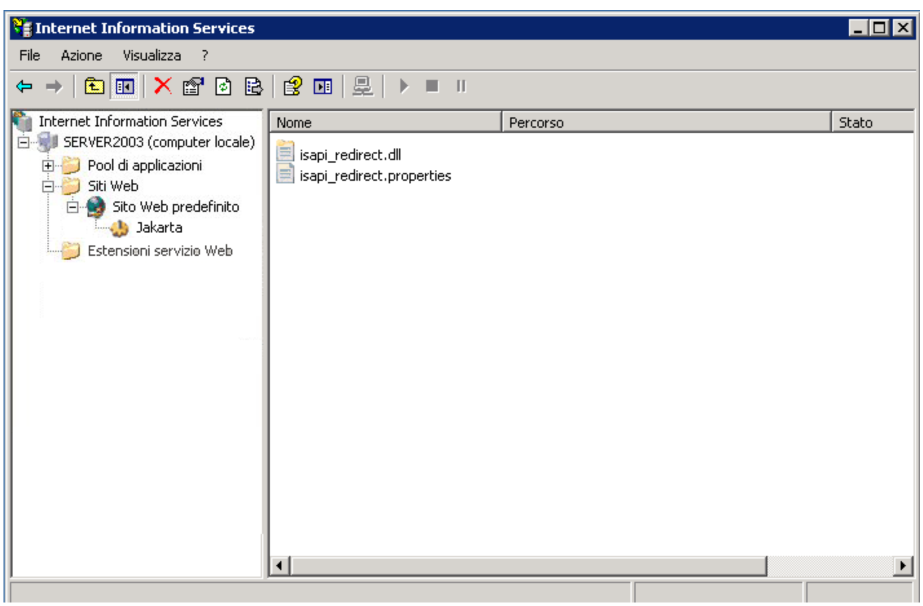
a Nel menu Start di Windows, aprire **Impostazioni** > **Pannello di controllo** > **Strumenti di amministrazione** >**Gestione Internet Information Services (IIS)**.

b Nel riquadro di destra, fare clic con il tasto destro su **<Nome computer locale>\Siti Web\<Nome sito Web>** e selezionare **Nuovo\Directory virtuale**.

c Assegnare alla directory il nome alias **Jakarta**, e impostare il percorso locale sulla directory contenente isapi_redirect.dll.

L'aspetto della finestra di gestione è simile a quella riportata di seguito:





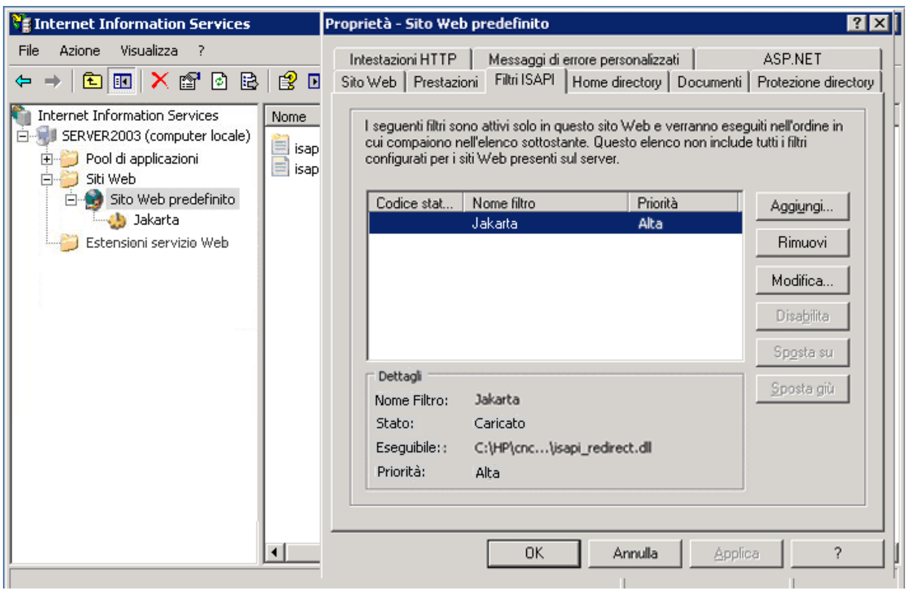
7 Aggiungere **isapi_redirect.dll** come filtro ISAPI.

a Fare clic con il tasto destro su <**Nome sito Web**> e selezionare **Proprietà**.

b Selezionare la scheda **Filtri ISAPI**, quindi fare clic sul pulsante **Aggiungi...**.

c Selezionare il Nome filtro **Jakarta**, e scorrere fino a **isapi_redirect.dll**. Viene aggiunto il filtro anche se ancora non è attivo.

L'aspetto della finestra di configurazione è simile a quella riportata di seguito:



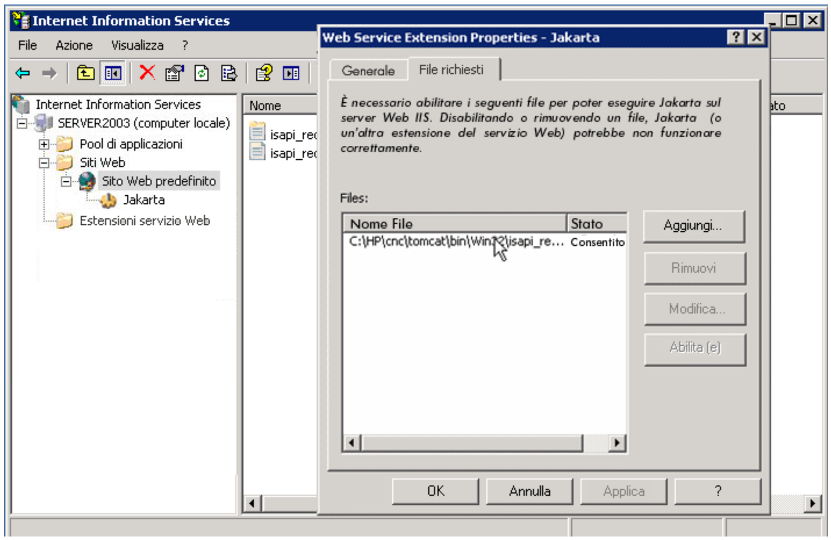
d Fare clic sul pulsante **Applica**.

8 Definire e consentire la nuova estensione del Servizio Web.

a Fare clic con il tasto destro su <**Nome computer locale**>**\Estensioni Servizio Web** e selezionare l'elemento del menu **Aggiungi nuova estensione Servizio Web...**.

b Assegnare il nome **Jakarta** alla nuova estensione Servizio Web, quindi scorrere fino al file **isapi_redirect.dll**.

Nota: prima di fare clic sul pulsante **OK**, selezionare la casella di controllo **Imposta lo stato dell'estensione su Consentito**.



9 Riavviare il Server Web IIS, e accedere all'applicazione tramite il Servizio Web.

Supporto IPv6

Configuration Manager supporta l'URL IPv6 solo per URL pubblici.

Per utilizzare Configuration Manager con un indirizzo IPv6:

1. Assicurarsi che il sistema operativo supporti IPv6 e IPv4. Per informazioni, consultare la documentazione relativa al sistema operativo.
2. Aprire il file **client-config.properties**, disponibile nella <**directory di installazione di Configuration Manager**>/**conf**, e modificare i seguenti valori:
   - Cambiare il valore del parametro **bsf.server.url** e assicurarsi che utilizzi il nome host. Ad esempio:

     bsf.server.url=http://mycomputer:8080/bsf
   - Cambiare il valore del parametro **bsf.server.services.url** e verificare che l'URL di Configuration Manager sia l'indirizzo del nome host. Ad esempio:

     bsf.server.services.url=http://<Configuration Manager host name>:
     <Configuration Manager Port>/bsf
3. Aprire il file Tomcat **servers\server-0\conf\server.xml** e modificare i seguenti valori:
   - Aggiungere l'indirizzo IPv6 all'hook SHUTDOWN aggiungendo **address**="**[::]**" al seguente tag:

     <Server port="8005" shutdown="SHUTDOWN" **address**="**[::]**" >
   - Duplicare il connettore HTTP. Per il secondo connettore, aggiungere l'indirizzo IPv6 [::]. Ad esempio:

```
<Connector port="8180" protocol="HTTP/1.1"
           connectionTimeout="20000"
           redirectPort="8443" />
<Connector port="8180" protocol="HTTP/1.1" address="[::]"
           connectionTimeout="20000"
           redirectPort="8443" />
```

➤ Duplicare il connettore AJP. Per il secondo connettore, aggiungere l'indirizzo IPv6 [::]. Ad esempio:

```
<Connector port="8009" protocol="AJP/1.3" redirectPort="8443"  address="[::]" />

<Connector port="8009" protocol="AJP/1.3" redirectPort="8443" />
```

4 Aggiungere la variabile ambientale al server: useIPv6="true":

Aprire il file **edit_server-0.bat**, disponibile nella <**directory di installazione di Configuration Manager**>**/bin**. Nella scheda Java, aggiungere la seguente proprietà alle opzioni Java: -DuseIPv6.

5 Riavviare il server.

LDAP

LDAP può essere configurato in Configuration Manager. Per informazioni, consultare "Impostazioni di sistema" nella Guida dell'utente di *HP Universal CMDB Configuration Manager*.

Protezione avanzata

Questa sezione include:

Nota: dopo l'aggiornamento, è necessario eseguire nuovamente la configurazione SSL. Per informazioni, consultare "Aggiornamento di Configuration Manager" a pagina 41.

Protezione avanzata Configuration Manager

Questa sezione introduce il concetto di applicazione Configuration Manager sicura ed esamina la pianificazione e l'architettura necessaria per implementare la protezione. Si consiglia vivamente di leggere questa sezione prima di procedere a esaminare la protezione avanzata presentata nelle seguenti sezioni.

Configuration Manager è progettato in modo da poter essere parte di un'architettura sicura, ed è quindi in grado di resistere alle minacce poste alla sicurezza a cui potrebbe essere esposto.

Le linee guida della protezione avanzata presentano la configurazione necessaria per poter implementare Configuration Manager in modo che abbia una protezione maggiore.

Le informazioni per la protezione avanzata offerta si riferiscono principalmente agli amministratori di Configuration Manager che devono familiarizzare con le impostazioni e raccomandazioni relative alla protezione avanzata prima di iniziare le procedure di protezione avanzata.

Di seguito sono illustrate le fasi preparatorie consigliate per la protezione avanzata del sistema:

- Valutare il rischio di protezione/stato della protezione per le reti generiche, e utilizzare le conclusioni quando si decide come integrare al meglio Configuration Manager nella rete.
- Sviluppare una buona conoscenza del framework tecnico di Configuration Manager e delle funzionalità di protezione di Configuration Manager.
- Riesaminare tutte le linee guida relative alla protezione avanzata.
- Verificare che Configuration Manager sia completamente funzionante prima di avviare le procedure di protezione avanzata.
- Seguire in ordine cronologico i passaggi delle procedure relative alla protezione avanzata in ciascuna sezione.

Importante:

- Le procedure di protezione avanzata si basano sul presupposto che si stanno implementando solo le istruzioni fornite in queste sezioni, e che non si stanno eseguendo altri passaggi relativi alla protezione avanzata documentati altrove.
- Laddove le procedure di protezione avanzata pongono l'attenzione su una particolare architettura distribuita, ciò non implica che questa sia l'architettura che meglio di adatta alle necessità dell'organizzazione.
- Si presume che le procedure incluse nelle seguenti sezioni siano stato eseguite su computer dedicati a Configuration Manager. L'uso del computer per scopi diversi oltre a Configuration Manager potrebbe determinare problemi.
- Le informazioni relative alla protezione avanzata fornite in questa sezione non sono intese come guida per la creazione della valutazione del rischio di protezione per i sistemi informatizzati.

Crittografare la password del database

La password del database è archiviata nel file <**Configuration Manager installation directory**>**\conf\database.properties**. Per crittografare la password, il nostro algoritmo di crittografia predefinito è conforme agli standard della FIPS 140-2.

La crittografia viene eseguito utilizzando una chiave, tramite la quale la password viene crittografata. La stessa chiave viene crittografata utilizzando un'altra chiave, conosciuta come chiave master. Entrambe le chiavi vengono crittografate utilizzando lo stesso algoritmo. Per informazioni sui parametri utilizzati nel processo di crittografia, consultare "Parametri di crittografia" a pagina 95.

Attenzione: se viene cambiato l'algoritmo di crittografia, tutte le password crittografate in precedenza non saranno più utilizzabili.

Per cambiare la crittografia della password del database:

1. Aprire la <**directory di installazione di Configuration Manager**>**\conf \encryption.properties** e modificare i seguenti campi:
   - ➤ **engineName.** Immettere il nome dell'algoritmo di crittografia.
   - ➤ **keySize.** Immettere la dimensione della chiave master per l'algoritmo selezionato.
2. Eseguire lo script **generate-keys.bat**, che crea la seguente directory: **cnc920\security\encrypt_repository** e generare la chiave di crittografia.
3. Eseguire l'utilità **bin\encrypt-password** per crittografare la password. Impostare il contrassegno **-h** per visualizzare le opzioni disponibili.
4. Copiare il risultato dell'utilità di crittografia della password e incollare la crittografia nel file **conf\database.properties**.

Parametri di crittografia

La seguente tabella elenca i parametri inclusi in **encryption.properties** utilizzato per la crittografia della password database. Per informazioni sulla crittografia della password database, consultare "Crittografare la password del database" a pagina 94.

Parametro	**Descrizione**
cryptoSource	Indica l'infrastruttura che implementa l'algoritmo di crittografia. Le opzioni disponibili sono: ➤ **lw.** Utilizza l'implementazione Bouncy Castle lightweight (opzione predefinita) ➤ **jce.** Java Cryptography Enhancement (infrastruttura di crittografia Java standard)
storageType	Indica il tipo di archivio chiavi. Attualmente, è supportato solo **file binario**.
binaryFileStorageName	Indica il punto nel file dove è archiviata la chiave master.
cipherType	Il tipo di crittografia. Attualmente, è supportato solo **symmetricBlockCipher**.
engineName	Il nome dell'algoritmo di crittografia. Sono disponibili le seguenti opzioni: ➤ **AES.** American Encryption Standard. Questa crittografia è conforme a FIPS 140-2. (opzione predefinita) ➤ **Blowfish** ➤ **DES** ➤ **3DES.** (conforme a FIPS 140-2) ➤ **Null.** Nessuna crittografia

Parametro	**Descrizione**
keySize	La dimensione della chiave master. La dimensione è determinata dall'algoritmo: ➤ **AES.** 128, 192, o 256 (opzione predefinita: 256) ➤ **Blowfish.** 0-400 ➤ **DES.** 56 ➤ **3DES.** 156
encodingMode	La codifica ASCII dei risultati di crittografia binari. Sono disponibili le seguenti opzioni: ➤ **Base64** (opzione predefinita) ➤ **Base64Url** ➤ **Hex**
algorithmModeName	La modalità dell'algoritmo. Attualmente, è supportato solo **CBC**.
algorithmPaddingName	L'algoritmo di spaziatura utilizzato. Sono disponibili le seguenti opzioni: ➤ **PKCS7Padding** (opzione predefinita) ➤ **PKCS5Padding**
jceProviderName	Il nome dell'algoritmo di crittografia JCE. **Nota:** rilevante solo quando crytpSource è **jce**. Per **lw**, è utilizzato engineName.

Attivare SSL sul Computer server con certificato autofirmato

Queste sezioni illustrano come configurare Configuration Manager per supportare l'autenticazione e la crittografia utilizzando il canale Secure Sockets Layer (SSL).

Configuration Manager utilizza Tomcat 7.0 come server applicazioni.

Nota: i percorsi delle directory e dei file dipendono da piattaforma specifica, sistema operativo e preferenze di installazione.

---

1 Prerequisiti

Prima di avviare la procedura seguente, rimuovere il file **tomcat.keystore** precedente posizionato nella **<directory di installazione di Configuration Manager>\java \lib\security\tomcat.keystore**.

2 Generare un Keystore server

Creare un keystore (tipo JKS) con un certificato autofirmato e corrispondente alla chiave privata:

➤ Dalla directory bin dell'installazione Java nella directory di installazione di Configuration Manager eseguire il seguente comando:

```
keytool -genkey -alias tomcat -keyalg RSA -keystore ..\lib\
security\tomcat.keystore
```

Si apre la finestra di dialogo della console.

➤ Immettere la password del keystore. Se la password è stata cambiata, cambiarla manualmente nel file.

➤ Rispondere alla domanda, **Quali sono nome e cognome?** Immettere il nome server Web Configuration Manager. Immettere gli altri parametri in relazione alla propria organizzazione.

- Immettere la password della chiave. La password della chiave DEVE essere la stessa della password keystore.

  Viene creato un keystore JKS con il nome **tomcat.keystore** con un certificato server con il nome **hpcert**.

3 Collocare il certificato nell'archivio dati attendibile del client

Aggiungere il certificato all'archivio dati attendibile del client in Internet Explorer sul computer (**Strumenti** > **Opzioni Internet** > **Contenuti** > **Certificati**). In caso contrario, verrà chiesto di eseguire questa procedura la prima volta che si tenta di utilizzare Configuration Manager.

Per informazioni sull'uso dei certificati client, consultare "Certificati client" a pagina 104.

Limitazione: in **tomcat.keystore** può essere presente un solo certificato server.

---

4 Verificare le impostazioni di configurazione del client

Aprire il file **client-config.properties**, posizionato nella directory **conf** della directory di installazione Configuration Manager. Impostare il protocollo di **bsf.server.url** su **https** e la porta su **8443**.

5 Modificare il file server.xml

Aprire il file **server.xml**, disponibile nella <**directory di installazione di Configuration Manager**>**\servers\server-0\conf**. Individuare la sezione che inizia con

Porta connettore="8443"

visualizzata nei commenti. Attivare lo script rimuovendo il delimitatore e aggiungendo i seguenti attributi al connettore HTTPS:

keystoreFile="<tomcat.keystore file location>" (consultare il passaggio 2 a pagina 97)
keystorePass="<password>"

Impostare come commento la seguente riga:

```
<Listener className="org.apache.catalina.core.AprLifecycleListener"
SSLEngine="on" />
```

6 Riavviare il server

7 Verificare la protezione del server

Per verificare che il server Configuration Manager sia protetto, immettere l'URL seguente nel browser Web: **https://Nome server o indirizzo ID di <Configuration Manager>:8443/cnc**.

Suggerimento: se non si riesce a stabilire una connessione, provare ad utilizzare un browser diverso o ad aggiornare il browser alla versione più recente.

Abilitare SSL sul computer server con un certificato dall'Autorità di certificazione

Per utilizzare un certificato emesso da un'Autorità di certificazione (CA), il keystore deve essere nel formato Java. L'esempio di seguito spiega come formattare il keystore per un computer Windows.

1 Prerequisiti

Prima di avviare la procedura seguente, rimuovere il file **tomcat.keystore** precedente posizionato nella **<directory di installazione di Configuration Manager>\java\lib \security\tomcat.keystore**.

2 Generare un Keystore server

a Generare un certificato CA firmato e installarlo in Windows.

b Esportare il certificato in un file ***.pfx** (incluse le chiavi private) utilizzando Microsoft Management Console (**mmc.exe**).

➤ Immettere qualsiasi stringa come la password per il file **pfx**. (Questa password viene chiesta quando si converte il tipo keystore in un keystore JAVA.)
Il file **.pfx** ora contiene un certificato pubblico e una chiave privata e la password è protetta.

c Copiare il file **.pfx** creato nella seguente cartella: <**directory di installazione di Configuration Manager**>**\java\lib\security**.

d Aprire il prompt dei comandi e cambiare la directory in <**directory di installazione di Configuration Manager**>**\bin\jre\bin**.

➤ Cambiare il tipo di keystore da **PKCS12** a un keystroke **JAVA** eseguendo il seguente comando:

```
keytool -importkeystore -srckeystore <directory di installazione di Configuration
Manager>\conf\security\<nome file pfx> -srcstoretype PKCS12 -destkeystore
tomcat.keystore
```

Viene chiesta l'origine della password keystrove (**.pfx**). È la password fornita durante la creazione del file pfx nel passaggio b.

3 Verificare le impostazioni di configurazione del client

Aprire il seguente file: <**Configuration Manager directory di installazione**> **\cnc\conf\client-config.properties** e verificare che la proprietà **bsf.server.url** sia impostata su **https** e la porta sia **8443**.

4 Modificare il file server.xml

Aprire il file **server.xml**, disponibile nella <**directory di installazione di Configuration Manager**>**\servers\server-0\conf**. Individuare la sezione che inizia con

```
Porta connettore="8443"
```

visualizzata nei commenti. Attivare lo script rimuovendo il delimitatore e aggiungendo le due righe seguenti:

```
keystoreFile="../../java/lib/security/tomcat.keystore"
keystorePass="password" />
```

Impostare come commento la seguente riga:

```
<Listener className="org.apache.catalina.core.AprLifecycleListener"
SSLEngine="on" />
```

5 Riavviare il server

6 Verificare la protezione del server

Per verificare che il server Configuration Manager sia protetto, immettere l'URL seguente nel browser Web: **https://Nome server o indirizzo ID di <Configuration Manager>:8443/cnc**.

Limitazione: in **tomcat.keystore** può essere presente un solo certificato server.

Nota: i percorsi delle directory e dei file dipendono da piattaforma specifica, sistema operativo e preferenze di installazione.

Ad esempio: java/{os name}/lib.

Abilitare SSL con un Certificato client

Se il certificato utilizzato dal server Web Configuration Manager è pubblicato da un'Autorità di certificazione (CA) conosciuta, molto probabilmente il browser Web è in grado di convalidare il certificato senza ulteriori azioni.

Se il CA non è ritenuto affidabile dall'archivio dati attendibile del server, importare il certificato CA nell'archivio dati attendibile del server.

Negli esempi seguenti viene illustrato come importare il certificato autofirmato **hpcert** nell'archivio dati attendibile del server (cacerts).

Per importare un certificato nell'archivio dati attendibile del server:

1. Sul computer client, individuare e rinominare il certificato **hpcert** in **hpcert.cer**.
2. Copiare **hpcert.cer** sul computer server nella <**directory di installazione di Configuration Manager**>**\java\bin**.
3. Sul server, importare il certificato nell'archivio dati attendibile CA (cacerts) utilizzando l'utilità keytool con il seguente comando:

   ```
   <directory di installazione di Configuration Manager>\java\bin\keytool.exe -
   import
   -alias hp -file hpcert.cer -keystore ..\lib\security\cacerts
   ```

4. Modificare il file **server.xml** (disponibile nella <**directory di installazione di Configuration Manager**>**\servers\server-0\conf**) come segue:
   - **a** Apportare le modifiche apportate nel passaggio 5 a pagina 98.
   - **b** Eseguire le modifiche, aggiungere i seguenti attributi al connettore HTTPS:

     ```
     truststoreFile="../../java/lib/security/cacerts"
     truststorePass="changeit" />
     ```

   - **c** Impostare clientAuth="true".
5. Verificare la protezione del server come descritto nel passaggio 7 a pagina 99.

Abilitare SSL solo per l'autenticazione

Questa attività descrive come configurare Configuration Manager per supportare solo l'autenticazione. È il livello minimo di protezione richiesto per lavorare con Configuration Manager.

1. Seguire uno dei passaggi per abilitare SSL sul computer server come descritto "Attivare SSL sul Computer server con certificato autofirmato" a pagina 97 fino al passaggio 6 a pagina 99 o "Abilitare SSL sul computer server con un certificato dall'Autorità di certificazione" a pagina 99 fino al passaggio 5 a pagina 101.
2. Immettere l'URL seguente nel browser Web: http://Nome server o indirizzo IP di <Configuration Manager>:8180/cnc.

Abilitare l'autenticazione del certificato client

Questa attività descrive come impostare Configuration Manager per accettare l'autenticazione del certificato lato client.

1. Seguire la procedura per abilitare SSL su un computer server come descritto in "Attivare SSL sul Computer server con certificato autofirmato" a pagina 97.
2. Aprire il seguente file: <**Configuration Manager directory di installazione**> **conf****lwssofmconf.xml.** Individuare la sezione che inizia con in-client certificate. Ad esempio:

   <in-clientCertificate userIdentifierRetrieveField="SubjectDN" userIdentifierRetrieveMode="FieldPart" userIdentifierRetrieveFieldPart="e" />

   Attivare la funzionalità certificato client rimuovendo il delimitatore.
3. Estrarre il nome utente dal certificato attenendosi alla seguente procedura:
   a. Il parametro **userIdentifierRetrieveField** indica quale campo certificato contiene il nome utente. Le opzioni possibili sono:
      - **SubjectDN**
      - **SubjectAlternativeName**

b Il parametro **userIdentifierRetrieveMode** indica se il nome utente è composto dall'intero contenuto del campo pertinente o solo da una parte di esso. Le opzioni possibili sono:

- **EntireField**
- **FieldPart**

c Se il valore di **userIdentifierRetrieveMode** è **FieldPart**, il parametro **userIdentifierRetrieveFieldPart** indica quale parte del campo pertinente costituisce il nome utente. Il valore è codificato con lettere seguendo la legenda definita nel certificato stesso.

4 Aprire il seguente file: **<Configuration Manager directory di installazione>\conf\client-config.properties** e modificare le seguenti proprietà:

- Cambiare **bsf.server.url** per utilizzare il protocollo HTTPS e cambiare la porta HTTPS con la porta descritta in "Attivare SSL sul Computer server con certificato autofirmato" a pagina 97.
- Cambiare **bsf.server.services.url** per utilizzare il protocollo HTTP e ripristinare la porta HTTP originale.

Certificati client

Questa sezione include:

Informazioni sul certificato client

Questa sezione descrive le informazioni del certificato client e come ottenere un identificatore utente da un certificato client.

- **Identificatore utente**

  L'identificatore utente è una parte unica delle informazioni ricevute dal certificato client utilizzato per identificare l'identità dell'utente.

➤ **Informazioni di base sul certificato client**

Le informazioni di base sul certificato client comprendono:

Campo certificato	**Descrizione**
Versione	La versione del certificato codificato. Esempio: 1 (0x1)
Numero di serie	Un numero intero positivo assegnato dall'autorità di certificazione a ciascun certificato. Esempio: 0 (0x0)
Algoritmo della firma	L'identificatore dell'algoritmo per l'algoritmo utilizzato dall'autorità di certificazione per firmare il certificato. Esempio: md5WithRSAEncryption
Autorità	L'entità che ha firmato e emesso il certificato. Esempio: CN=Issuer, C=US, ST=NY, L=New York, O=Work Organization, O=example.com
Validità	Il periodo di tempo durante il quale l'autorità di certificazione garantisce la conservazione delle informazioni relative allo stato del certificato: ➤ **No prima di**. Specifica la data di inizio del periodo di validità del certificato. Esempio: Nov 25 04:34:49 2009 GMT ➤ **No oltre il**. Specifica la data di fine del periodo di validità del certificato. Esempio: Nov 25 04:34:49 2010 GMT

Campo certificato	Descrizione
Oggetto	L'entità associata con la chiave pubblica archiviata nel campo chiave pubblica oggetto.
Informazioni sulla chiave pubblica dell'oggetto	Utilizzate per trasferire la chiave pubblica e identificare l'algoritmo con il quale è utilizzata la chiave (ad esempio, RSA, DSA o Diffie-Hellman).

Per ulteriori informazioni, consultare Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile:

http://tools.ietf.org/html/rfc5280

➤ Campo oggetto

Il campo oggetto (che prende anche il nome di Subject Distinguish Name o SubjectDN) identifica l'entità associata con la chiave pubblica.

Il campo oggetto contiene i seguenti attributi pertinenti (può contenere anche altri attributi):

Attributo oggetto	Descrizione attributo oggetto	Esempio
CN	Nome comune	CN=Bob BobFamily
emailAddress	Indirizzo e-mail	*emailAddress=bob@example.com*
C	Nome paese	C=US
ST	Nome stato o provincia	ST=NY
L	Nome località	L=New York
O	Nome organizzazione	O=Work Organization
OU	Nome unità organizzativa	OU=Managers

Per recuperare l'identificatore utente dall'oggetto, è possibile utilizzare l'intero campo SubjectDN o l'attributo SubjectDN.

➤ Estensione delle informazioni sul certificato client

Le estensioni definite per i certificati X.509 v3 offrono i metodi per l'associazione di attributi aggiuntivi con gli utenti o le chiavi pubbliche e per la gestione delle relazioni tra le autorità di certificazione. Il Campo nome alternativo oggetto può contenere l'identificatore utente.

➤ Campo nome alternativo oggetto

L'estensione del nome alternativo dell'oggetto consente di vincolare le identità all'oggetto del certificato. Queste identità possono essere incluse in aggiunta a o in sostituzione dell'identità nel campo oggetto del certificato.

Il campo nome alternativo dell'oggetto può contenere le seguenti identità:

Identità	**Esempio**
otherName	Altro nome: Nome principale= *bobOtherAltName@example.com*
rfc822Name	Nome RFC822=*bobRFC822AltName@example.com*
dNSName	Nome DNS=example1.com
x400Address	
directoryName	Indirizzo directory: E=*bobDirAltName@example.com*, CN=bob, OU=Gold Ballads, O=Gold Music, C=US
ediPartyName	
uniformResourceIdentifier	URL=http://example.com/
iPAddress	Indirizzo IP=192.168.7.1
registeredID	ID registrato=1.2.3.4

Per recuperare l'identificatore utente dal nome alternativo dell'oggetto è possibile utilizzare una delle identità.

Configurazione

Configuration Manager utilizza LW-SSO per sfruttare l'identificatore utente da un certificato client. I seguenti attributi vengono utilizzati dal gestore del certificato client per configurare LW-SSO in modo da sfruttare l'identificatore client:

Per sfruttare le informazioni dal certificato client, Configuration Manager deve essere configurato in modo da recuperare l'identificatore utente.

Devono essere decisi i seguenti elementi:

- Quale campo deve essere utilizzato: SubjectDN o Nome alternativo oggetto?
- Deve essere utilizzato l'intero campo o solo una parte?
- Se viene utilizzata una parte del campo di input, specificare un valore: fornire l'attributo oggetto per SubjectDN o l'identità per Nome alternativo oggetto.

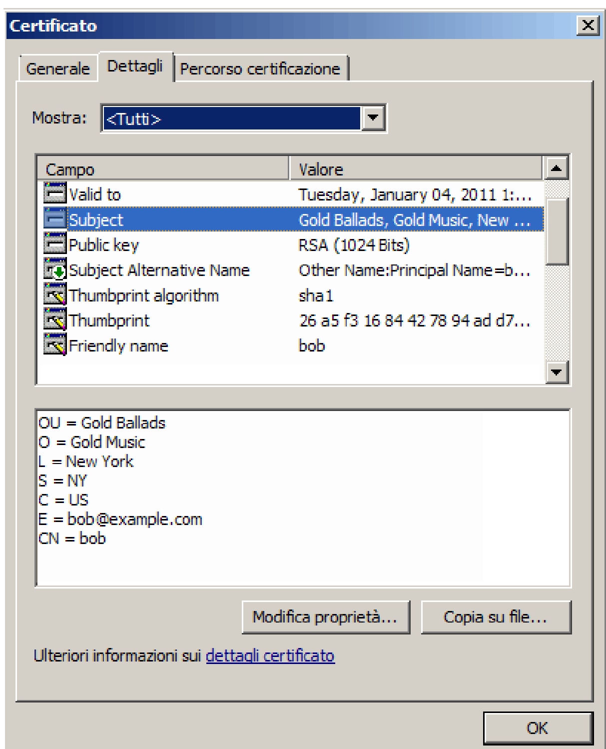
I seguenti attributi devono essere utilizzati dal gestore del certificato client per configurare LW-SSO:

Nome attributo	Descrizione
enabled	Specifica se il gestore è abilitato o disabilitato. **Importante**: si consiglia vivamente di impostare in modo esplicito il valore su false e abilitare il gestore solo quando è necessaria la convalida del certificato client.
userIdentifierRetrieveField	Il parametro indica quale campo certificato contiene l'identificatore utente. Le opzioni sono: **SubjectDN** o **SubjectAlternativeName**.
userIdentifierRetrieveMode	Il parametro userIdentifierRetrieveMode indica se l'identificatore utente è composto dall'intero contenuto del campo pertinente o solo una parte di esso. Le opzioni sono: **EntireField** o **FieldPart**.

Nome attributo	**Descrizione**
userIdentifierRetrieveFieldPart	Se il valore di **userIdentifierRetrieveMode** è **FieldPart**, il parametro indica quale parte del campo pertinente costituisce il nome utente. Il valore è codificato con lettere seguendo la legenda definita nel certificato stesso **Nota**: questo attributo non può essere vuoto quando **userIdentifierRetrieveMode** è impostato su **FieldPart**. Inoltre, non può essere vuoto quando **userIdentifierRetrieveField** è impostato su **SubjectAlternativeName**.

Esempi

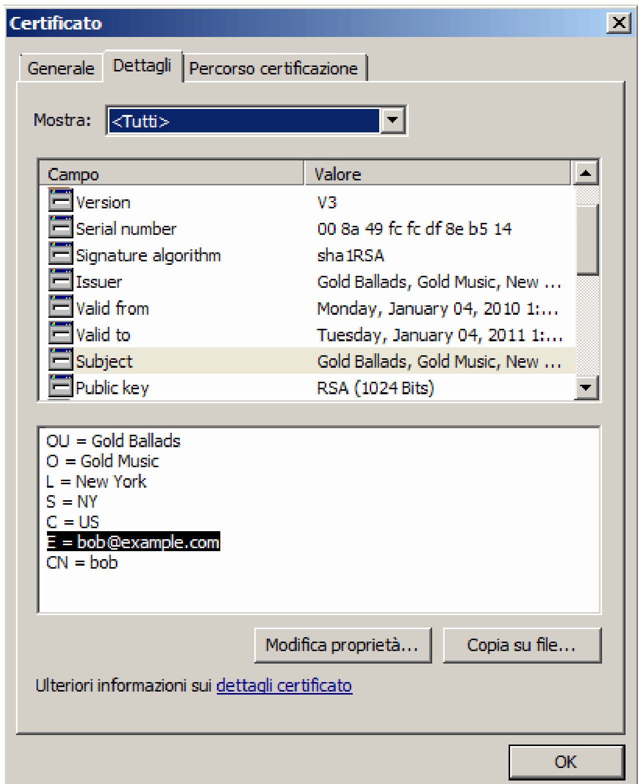
➤ L'oggetto è utilizzato per conservare l'identificatore utente



L'esempio di seguito mostra come configurare il gestore per ottenere l'identificatore utente dall'intero SubjectDN:

```
<in-clientCertificate userIdentifierRetrieveField="SubjectDN"
userIdentifierRetrieveMode="EntireField" />
```

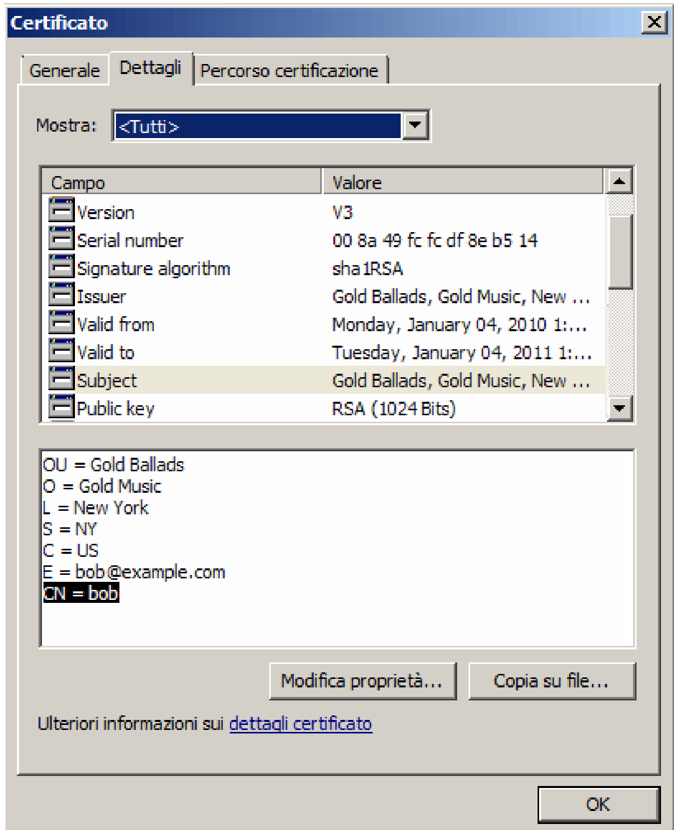
➤ **Il campo E-mail dell'oggetto è utilizzato per conservare l'identificatore utente**



Utilizzare i nomi dei campi visualizzati nella legenda del certificato client. L'esempio di seguito mostra come configurare il gestore per ottenere l'identificatore utente dal campo e-mail dell'oggetto:

```
<in-clientCertificate userIdentifierRetrieveField="SubjectDN"
userIdentifierRetrieveMode="FieldPart" userIdentifierRetrieveFieldPart="E" />
```

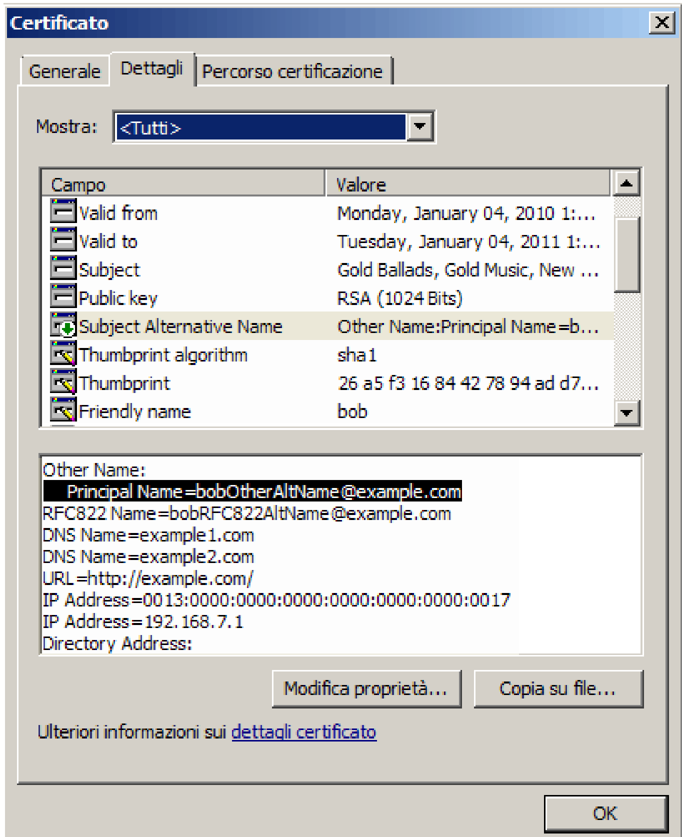
➤ Il campo Nome comando dell'oggetto è utilizzato per conservare l'identificatore utente



Utilizzare i nomi dei campi visualizzati nella legenda del certificato client. L'esempio di seguito mostra come configurare il gestore per ottenere l'identificatore utente dal campo Nome comando dell'oggetto:

```
<in-clientCertificate userIdentifierRetrieveField="SubjectDN"
userIdentifierRetrieveMode="FieldPart" userIdentifierRetrieveFieldPart="CN" />
```

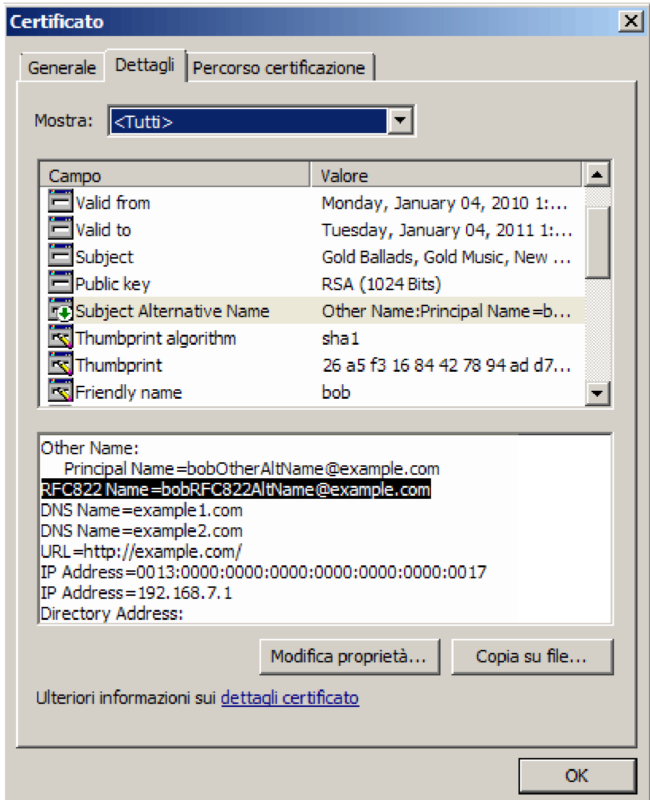
➤ **L'identità otherName del Nome alternativo oggetto è utilizzato per conservare l'identificatore utente**



Utilizzare il nome dell'identità visualizzato nella legenda del certificato client. L'esempio di seguito mostra come configurare il gestore per ottenere l'identificatore utente dall'identità otherName del Nome alternativo oggetto:

```
<in-clientCertificate userIdentifierRetrieveField="SubjectAlternativeName"
userIdentifierRetrieveMode="FieldPart" userIdentifierRetrieveFieldPart="Principal
Name" />
```

➤ **L'identità rfc822Name del Nome alternativo oggetto è utilizzato per conservare l'identificatore utente**



Utilizzare il nome dell'identità visualizzato nella legenda del certificato client. L'esempio di seguito mostra come configurare il gestore per ottenere l'identificatore utente dall'identità rfc822Name del Nome alternativo oggetto:

```
<in-clientCertificate userIdentifierRetrieveField="SubjectAlternativeName"
userIdentifierRetrieveMode="FieldPart" userIdentifierRetrieveFieldPart="Principal
Name" />
```

Configurazione di Configuration Manager per utilizzare UCMDB con SSL

È possibile configurare Configuration Manager per utilizzare UCMDB con Secure Sockets Layer (SSL). Il connettore SSL sulla porta 8443 è abilitato per impostazione predefinita in UCMDB.

Per esportare il certificato server e importarlo nel truststore del client

1. Passare alla <**directory di installazione di UCMDB**>**bin****jre****bin** ed eseguire il seguente comando:

   ```
   keytool -export -alias hpcert -keystore <UCMDB server dir>
   \conf\security\server.keystore  -storepass hppass -file <certificatefile>
   ```

2. Importare il certificato nel truststore di Configuration Manager (il truststore jre predefinito):

   ```
   <CM_JAVA_HOME>\bin\keytool -import -trustcacerts -alias hpcert -keystore
   <CM_JAVA_HOME>\lib\security\cacerts -storepass changeit -file
   <certificatefile>
   ```

3. Impostare le proprietà di connessione di UCMDB in Configuration Manager:

   Passare a **Sistema** > **Impostazioni** > **Integrazioni** > **UCMDB Foundation** > **UCMDB Foundation.** Impostare il metodo di connessione su **HTTPS**, la porta del server UCMDB sulla porta HTTPS di UCMDB e impostare l'URL di accesso a UCMDB su https://<HostName>:8443.

4. Salvare il set di configurazione e attivarlo. Riavviare Configuration Manager.

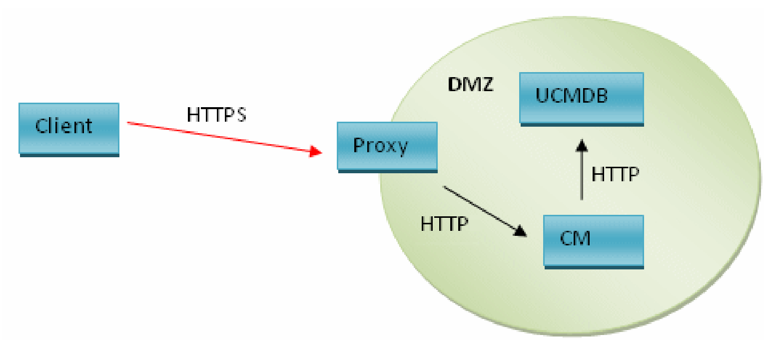
Per configurare Configuration Manager in modo da operare con altri prodotti (ad esempio bilanciamenti del carico) utilizzando Secure Sockets Layer (SSL), importare il certificato di protezione del prodotto nel truststore di Configuration Manager (truststore jre predefinito) eseguendo il seguente comando:

```
<CM_JAVA_HOME>\bin\keytool -import -trustcacerts -alias <alias> -keystore
<CM_JAVA_HOME>\lib\security\cacerts -storepass changeit -file <certificatefile>
```

Proxy inverso

Quando Configuration Manager e UCMDB risiedono in un DMZ, si consiglia di configurare il sistema in modo che funzioni con un server proxy inverso. Le procedure di configurazione sono identiche a quelle per la configurazione di UCMDB in modo che funzioni con un proxy inverso. Per abilitare l'accesso a Configuration Manager è necessario eseguire la mappatura dei percorsi **/cnc** e **/bsf** sugli URL del server remoto dove è installato Configuration Manager.

L'immagine di seguito mostra il processo di configurazione per un proxy inverso per Configuration Manager:



Ad esempio, se il proxy inverso è un server Apache, aggiunge le seguenti righe al file **Apache2.2\conf\extra\httpd-ssl.conf** e riavviare il server Apache:

```
ProxyPass /cnc http://<CM_HOSTNAME>:<CM_HTTP_PORT>/cnc
ProxyPassReverse /cnc http:// <CM_HOSTNAME>:<CM_HTTP_PORT>/cnc
ProxyPass /bsf http://< CM_HOSTNAME >:<CM_HTTP_PORT>/bsf
ProxyPassReverse /bsf http:// <CM_HOSTNAME>:<CM_HTTP_PORT>/bsf
```

Diversi tipi di proxy inverso possono richiedere procedure differenti per la configurazione, per ulteriori informazioni consultare la documentazione del server proxy.

Per configurare un proxy inverso per Configuration Manager:

Aggiornare il file **client-config.properties** nella <**directory di installazione di Configuration Manager**>**\conf** come segue:

```
bsf.server.url=https://<proxy-server-name>:443/bsf
```

La porta HTTPS predefinita del proxy Apache è 443.

Parte II

Appendici

A

Limitazioni sulla capacità

La tabella di seguito elenca i limiti di capacità per Configuration Manager.

Numero massimo di viste	100
Numero massimo di criteri	300
Numero massimo di CI compositi per vista	5000
Numero massimo di utenti simultanei	50
Numero massimo di CI compositi nel modulo Analisi configurazione	1000

B

Autenticazione Lightweight Single Sign-On (LW-SSO) – Riferimenti generali

Questo capitolo comprende:

Panoramica dell'autenticazione LW-SSO

LW-SSO è un metodo di controllo degli accessi che consente a un utente di effettuare l'accesso una sola volta per accedere alle risorse di più sistemi software senza che vengano richieste di nuovo le credenziali. Le applicazioni del gruppo di sistemi software configurato considerano l'autenticazione attendibile. Non è pertanto necessario procedere a ulteriori autenticazioni quando ci si sposta da un'applicazione all'altra.

Le informazioni in questa sezione si applicano alla versione 2.2 e 2.3 di LW-SSO.

Per informazioni sulla risoluzione dei problemi relativi a LW-SSO, consultare "LW-SSO - Risoluzione dei problemi e limitazioni" a pagina 141.

Questa sezione comprendere i seguenti argomenti:

Scadenza del token LW-SSO

Il valore di scadenza del token LW-SSO determina la validità della sessione dell'applicazione. Quindi, il valore di scadenza deve essere almeno uguale al valore di scadenza della sessione dell'applicazione.

Configurazione consigliata della Scadenza del token LW-SSO

La scadenza del token deve essere configurata per ciascuna applicazione che utilizza LW-SSO. Il valore consigliato è 60 minuti. Per un'applicazione che non richiede un valore elevato di protezione, è possibile configurare un valore di 300 minuti.

Orario GMT

Tutte le applicazioni comprese in una integrazione LW-SSO devono utilizzare lo stesso orario GMT con una differenza massima di 15 minuti.

Funzionalità multi-dominio

La Funzionalità multi-dominio richiede che per tutte le applicazioni dell'integrazione LW-SSO vengano configurate le impostazioni trustedHosts (o le impostazioni **protectedDomains**), se le applicazioni dovranno integrarsi con applicazioni di domini DNS differenti. Inoltre, è necessario aggiungere il dominio corretto nell'elemento **lwsso** della configurazione.

Ottenere il SecurityToken per la funzionalità URL

Per ricevere le informazioni inviate come **SecurityToken per URL** da altre applicazioni, per l'applicazione host deve essere configurato il dominio corretto nell'elemento **lwsso** della configurazione.

Avvisi di protezione LW-SSO

In questa sezione vengono descritti gli avvisi di protezione correlati alla configurazione LW-SSO:

- **Parametro InitString riservato in LW-SSO.** LW-SSO utilizza la crittografia simmetrica per convalidare e creare un token LW-SSO. Il parametro **initString** della configurazione viene utilizzato per l'inizializzazione della chiave segreta. Un'applicazione crea un token e ciascuna applicazione che utilizza lo stesso parametro initString lo convalida.

  Attenzione:

  - Non è possibile utilizzare LW-SSO senza impostare il parametro **initString**.
  - Il parametro **initString** indica informazioni riservate e deve essere considerato riservato in termini di pubblicazione, trasporto e persistenza.
  - Il parametro **initString** deve essere condiviso solo tra applicazioni che si integrano tra loro mediante LW-SSO.
  - Il parametro **initString** deve avere una lunghezza minima di 12 caratteri.

- **Abilita LW-SSO solo se necessario.** LW-SSO deve essere disabilitato a meno che non venga richiesto specificatamente.
- **Livello di protezione autenticazione.** L'applicazione che utilizza il framework di autenticazione più debole e rilascia un token LW-SSO che è considerato affidabile dalle altre applicazioni integrate determina il livello di protezione delle autenticazioni per tutte le le altre applicazioni.

  Si raccomanda che soltanto le applicazioni che utilizzano un framework di autenticazione protetto rilascino un token LW-SSO.

- **Implicazioni crittografia simmetrica.** LW-SSO utilizza la crittografia simmetrica per rilasciare e convalidare i token LW-SSO. Quindi, qualsiasi applicazione che utilizza LW-SSO può rilasciare un token da rendere attendibile per tutte le altre applicazioni che condividono lo stesso parametro **initString**. Questo rischio potenziale è importante quando un'applicazione condivide un initString sia residente su, o accessibile da una posizione non attendibile.
- **Mappatura utente (Sincronizzazione).** Il framework LW-SSO non garantisce la mappatura utente tra le applicazioni integrate. Quindi, l'applicazione integrata deve monitorare la mappatura utente. Si consiglia di condividere lo stesso registro utente (ad esempio LDAP/AD) tra tutte le applicazioni integrate.

  L'impossibilità di eseguire la mappatura degli utenti può causare violazioni della protezione e comportamenti negativi dell'applicazione. Ad esempio, si potrebbe assegnare lo stesso nome utente a diversi utenti reali in varie applicazioni.

  Inoltre, nei casi in cui un utente esegue l'accesso a un'applicazione (AppA) e successivamente accede a una seconda applicazione (AppB) che utilizza l'autenticazione contenitore o applicazione, l'impossibilità di eseguire la mappatura dell'utente forzerà l'utente stesso ad accedere manualmente all'AppB e ad inserire un nome utente. Se l'utente inserisce un nome utente diverso da quello utilizzato per l'accesso all'AppA, si può verificare il seguente comportamento: se l'utente, successivamente, accede ad una terza applicazione (AppC) dall'AppA o AppB, dovrà accedere utilizzando gli stessi nomi utente utilizzanti per l'accesso all'AppA o AppB rispettivamente.
- **Gestione identità**. Utilizzato per scopi di autenticazione, tutte le risorse non protette nella Gestione identità devono essere configurate con l'impostazione **nonsecureURLs** nel file di configurazione LW-SSO.

C

Risoluzione dei problemi

Questo capitolo comprende:

Risoluzione dei problemi generali e limitazioni

Limitazioni

I nuovi tipi di CI creati in UCMDB non saranno visualizzati fino a quando non viene disconnesso Configuration Manager ed eseguito nuovamente l'accesso.

Risoluzione dei problemi

Problema. L'attributo **nome** del tipo CI nodo non è qualificato come cambiamento monitorato, e non è stato copiato nello stato autorizzato durante l'autorizzazione del CI. Si verifica se è installata la Configuration Manager versione 9.20 senza Content Pack 9 per UCMDB.

Soluzione. Procedere con una delle seguenti operazioni:

- Impostare manualmente l'attributo **nome** per essere qualificato come cambiamento monitorato in Gestione tipo CI di UCMDB.
- Installare il Content Pack 9.

Problema. Quando viene installato il servizio Configuration Manager, viene visualizzato il seguente messaggio di errore:

> Windows could not start the HP Universal CMDB Configuration Manager on Local Computer. For more information, review the System Manager Event log. If this is a non-Microsoft service, contact the service vendor, and refer to service-specific error code 0.

Soluzione. Procedere come segue:

1. Passare alla **<directory di installazione di Configuration Manager >\cnc\bin** ed eseguire il seguente comando:

   `edit-server-0.bat`

2. Selezionare la scheda Avvio. Nell'elenco a discesa Modalità (in basso), selezionare **jvm** al posto di **exe**.
3. Selezionare la scheda Spegnimento. Nel campo Classe, cambiare il cognome da **Boostrap** a **Bootstrap**.
4. Fare clic su **OK**.
5. Eseguire il servizio.

Gestione distribuzione - Risoluzione dei problemi e limitazioni

Per la risoluzione dei problemi relativi a Gestione distribuzione, aprire il registro sessione dalla sessione precedente, disponibile nella seguente directory:

%temp%\HP\ucmdb-dm\Workspace\Sessions

Linee guida generali per la ridistribuzione

Durante l'installazione, nella pagina Convalida di Gestione distribuzione vengono visualizzati degli avvisi ed errori facendo clic sul pulsante dettagli accanto a ciascun componente distribuito.

Una volta individuato il problema durante la distribuzione e trovata una soluzione, eseguire le seguenti operazioni:

1. Disinstallare i prodotti distribuiti e riavviare il computer.
2. Riavviare Gestione distribuzione e inserire nuovamente tutte le configurazioni.

Problemi legati agli errori di distribuzione

Problema. Errore di autorizzazione durante la distribuzione.

Il registro sessione indica la presenza di un problema con le autorizzazioni utente del database durante la creazione di un nuovo schema.

Soluzione. Per creare un nuovo database, è necessario disporre delle relative autorizzazioni. Verificare che le credenziali utente utilizzate nella distribuzione siano sufficienti per spazio colonna e creazione schema.

Problema. Errore nella creazione dello schema/database in UCMDB.

Il registro sessione indica che Gestione distribuzione non è riuscito a creare uno schema o database.

Soluzione:

Nota: Si noti che non è possibile creare un nuovo schema UCMDB e connettersi a uno schema cronologia UCMDB esistente (senza considerare il tipo di server database).

Verificare che lo schema di UCMDB e lo schema cronologia di UCMDB non utilizzino il seguente tipo di connessione:

- Schema UCMDB - Crea nuovo schema
- Schema cronologia di UCMDB - Connetti a schema esistente

Problema. Errore nella creazione dello schema/database in UCMDB.

Il registro sessione indica che lo schema non può essere creato.

Soluzione. Aprire session.log e individuare il seguente messaggio:
Errore SQL esecuzione dichiarazione CREATE USER <nome schema>

Quando si assegna un nome allo schema Oracle nella pagina Configurazione database di Gestione distribuzione, utilizzare esclusivamente le lettere (a-z), le cifre (0-9) e il segno meno ('-').

Problema. Impossibile creare lo schema perché lo spazio è insufficiente.

Soluzione. Aumentare la quantità di spazio libero sullo schema o database. Utilizzare le interfaccia di gestione standard offerte da Oracle e Microsoft.

Problema. Configurazione del database non riuscita con il seguente errore:
NT AUTHORITY\ANONYMOUS LOGON – Impossibile connettersi al database.

Quando si seleziona un server MSSQL con autenticazione NTLM per la configurazione di un database UCMDB, la configurazione del database non riesce causando un errore di distribuzione.

Soluzione. Distribuire UCMDB su un computer localhost (unico punto dove è supportata l'autenticazione NTLM).

Problema. Errore nella configurazione del database di Configuration Manager durante la creazione di un nuovo database.

Nel riquadro dettagli di Gestione distribuzione possono essere visualizzati i seguenti errori:

```
Failed to create Oracle schema due to error: ORA-01031: insufficient privileges
```

oppure

```
Failed to create a schema to the database: machineName.
Reason: ORA-01919: role 'RESOURCE' does not exist
```

Soluzione. Verificare che l'utente del database disponga dei seguenti privilegi del ruolo:

- Connetti
- Risorsa

Problema. Impossibile eseguire la distribuzione. Spazio su disco insufficiente nel computer host di destinazione.

Soluzione. Accedere al computer host di destinazione e verificare che sia disponibile spazio a sufficienza per la distribuzione:

- UCMDB richiede 1GB di spazio
- Configuration Manager richiede 1GB di spazio
- DDMA richiede 1GB di spazio

Nota: Oltre ai requisiti specifici del prodotto, è necessario anche un 1GB di spazio libero per la gestione dei file temporanei.

Problema. Ping dell'utilità UCMDB non riuscito.

Questa utilità viene eseguita dal computer Configuration Manager e verifica la disponibilità della connessione verso l'istanza UCMDB esistente. Aprire session.log e individuare il seguente messaggio:
Failed to test connection due to error: java.net.ConnectException: Connection refused: connect.

Soluzione:

- Verificare che la porta 8080 su UCMDB di destinazione non sia bloccata dal firewall di Windows.
- verificare che il server UCMDB sia accessibile dal computer Configuration Manager, e che la distribuzione di UCMDB sia completata, attiva e in esecuzione.

Connessione computer host non disponibile

Problema. RPC non disponibile o errore sconosciuto.

Premendo il pulsante Test connessione si verifica l'errore RPC non disponibile.

Soluzione. Correggere il nome host se non corretto, e verificare che il servizio WMI e i servizi Server siano in esecuzione e che il firewall di Windows non stia bloccando l'accesso all'interfaccia WMI.

Disabilitare il firewall di Windows o aggiungere un'eccezione firewall abilitando l'accesso all'amministrazione remota.

Per eseguire questa operazione, aprire il pannello di controllo **Firewall** e selezionare **Regole connessioni in entrata.** Abilitare tutti i File e stampanti, regole WMI e la porta 8080.

Test connessione non riuscito

Problema. Accesso negato.

L'accesso è negato a causa di un nome utente o password errati, impostazioni DNS non valide o perché il nome utente utilizzato nella distribuzione non dispone di credenziali di amministrazione sul computer host di destinazione.

Soluzione. Verificare che le credenziali utente specificate siano corrette e che l'utente disponga delle credenziali di amministrazione sul computer host di destinazione.

Impossibile accedere all'applicazione

Problema. Al termine della distribuzione – accesso all'applicazione non riuscito (UCMDB o Configuration Manager).

Soluzione. Verificare che i seguenti servizi di UCMDB e Configuration Manager esistano e siano in esecuzione.

- Servizio **UCMDB_Server**
- Servizio **HPUCMDBCMoasisSNAPSHOTserver0**

Riesaminare i registri di distribuzione nella directory delle sessioni per eventuali errori.

LW-SSO è disabilitato

Problema. Distribuzione eseguita - funzionalità LW-SSO disabilitata.

Soluzione. Verificare che la stringa di inizializzazione di LW-SSO e il dominio siano identici su UCMDB e Configuration Manager (e OO, se applicabile).

Riesaminare le impostazioni di configurazione di LW-SSO nei prodotti tramite i seguenti metodi:

- Configuration Manager – Aprire il file **lwssofmconf.xml** e verificare le definizioni di dominio e stringa di inizializzazione. Il file è disponibile nella <**directory di installazione di Configuration Manager** >**\conf**.
- UCMDB – Aprire UCMDB e selezionare **Gestioni** > **Amministrazione** > **Gestione impostazioni infrastruttura**.

Se sia Configuration Manager che UCMDB risiedono su computer host che hanno domini DNS diversi, verificare che le impostazioni **Domini attendibili** includano i domini DNS e siano abilitate su entrambi i prodotti.

Per ulteriori informazioni relative alla distribuzione, la Gestione distribuzione può essere abilitata in modalità debug. La modalità debug offre ulteriori informazioni relative alla distribuzione.

Per abilitare la modalità debug:

1. Una volta eseguita la Gestione distribuzione, aprire la finestra del browser e inserire %temp% nella barra degli indirizzi.
2. Scorrere fino alla cartella **hp\ucmdb-dm**.
3. Aprire il file **ini** nell'editor di testo e aggiungere la seguente proprietà all'ultima riga del file:

   –Ddebug.mode=true
4. Utilizzare **%temp%\HP\ucmdb-dm\ucmdb-dm.exe** per eseguire Gestione distribuzione.

Accesso a Configuration Manager - Risoluzione dei problemi e limitazioni

Limitazioni

➤ Tutte le volte che viene cambiato l'orario sul server Tomcat di Configuration Manager, il server deve essere riavviato per poter aggiornare l'ora sul server.

Risoluzione dei problemi

Problema. Dopo avere cambiato il set di configurazione in **Sistema** > **Impostazioni**, il server non si avvia.

Soluzione. Tornare al set di configurazione precedente. Procedere come segue:

1. Eseguire questo comando per individuare l'ID dell'ultimo set di configurazione attivato:

   <directory di installazione di Configuration Manager >\bin\export-cs.bat <proprietà database> --history

dove <**proprietà database**> può essere specificato per puntare sulla posizione della <**directory di installazione di Configuration Manager**>**conf**\
database.properties o specificando ciascuna proprietà del database. Ad esempio:

```
cd <directory di installazione di Configuration Manager>\bin export-cs.bat -
p ..\conf\database.properties --history
```

2 Eseguire questo comando per esportare l'ultimo set di configurazione:

```
<directory di installazione di Configuration Manager>\bin\export-cs.bat
<proprietà database> <ID set di configurazione> <nome file dump>
```

dove <**ID set di configurazione**> è l'ID set di configurazione dal passaggio precedente e <**file dump**> è il nome di un file temporaneo utilizzato per salvare il set di configurazione. Ad esempio, per esportare il set di configurazione con l'ID **491520** sul file **mydump.zip**, immettere:

```
cd <directory di installazione di Configuration Manager>\bin export-cs.bat -
p ..\conf\database.properties -i 491520 -f mydump.zip
```

3 Interrompere l'esecuzione del servizio Configuration Manager.

4 Eseguire questo comando per importare e attivare il set di configurazione precedente:

```
<directory di installazione di Configuration Manager >\bin\import-cs.bat
<proprietà database> -i <nome file dump> --activate
```

Problema. Si è verificato un errore nella connessione UCMDB.

Soluzione. La causa potrebbe essere una delle seguenti:

➤ Il server UCMDB è spento. Riavviare Configuration Manager una volta attivato completamente UCMDB (verificare che lo stato del server UCMDB sia **Attivo**).

➤ Il server UCMDB è attivo ma le credenziali di connessione a Configuration Manager o l'URL sono errate. Avviare Configuration Manager. Selezionare **Sistema** > **Impostazioni** > **Integrazioni** > **UCMDB Foundation** > **UCMDB Foundation**, cambiare le impostazioni e salvare il nuovo set di configurazione. Attivare il set di configurazione e riavviare il server.

Problema. Le impostazioni di connessione LDAP sono errate.

Soluzione. Tornare al set di configurazione precedente. Impostare le impostazioni di connessione LDAP corrette e attivare il nuovo set di configurazione.

Problema. I cambiamenti al modello classe UCMDB non vengono rilevati in Configuration Manager.

Soluzione. Riavviare il server Configuration Manager.

Problema. Il registro di Configuration Manager contiene un errore **Timeout esecuzione UCMDB scaduto**.

Soluzione. Si verifica quando il database UCMDB è sovraccarico. Per correggere il problema, aumentare il timeout di connessione nel modo seguente:

1 Creare un file jdbc.properties all'interno della cartella **UCMDBServer\conf**.
2 Immettere il seguente testo: QueryTimeout=<numero in secondi>.
3 Riavviare il server UCMDB.

Problema. Configuration Manager non consente di aggiungere un vista da gestire.

Soluzione. Quando viene aggiunta una vista da gestire, in UCMDB viene creato un nuovo TQL. Se viene raggiunto il limite massimo di TQL attivi, non è possibile aggiungere la vista. Aumentare il limite dei TQL attivi in UCMDB cambiando le seguenti impostazioni in Gestione impostazioni infrastruttura:

- Numero massimo di TQL attivi nel server
- Numero massimo di TQL cliente attivi

Problema. Il certificato del server HTTPS non è valido.

Soluzione. La causa potrebbe essere una delle seguenti:

- ➤ La data di validità del certificato è scaduta. È necessario ottenere un nuovo certificato.
- ➤ L'autorità di certificazione del certificato non è un'autorità affidabile. Aggiungere l'autorità del certificato all'elenco Autorità di certificazione principale attendibile.

Problema. Quando si esegue l'accesso dalla pagina di accesso di Configuration Manager, si riceve un errore di accesso o l'accesso alla pagina è negato.

Soluzione. La causa potrebbe essere una delle seguenti:

- ➤ Il nome utente potrebbe non essere stato definito nel fornitore dell'autenticazione (LDAP esterno/condiviso). Aggiungere l'utente nel sistema Fornitore autenticazione.
- ➤ L'utente è stato definito ma non possiede l'autorizzazione per l'accesso per Configuration Manager. Concedere all'utente l'autorizzazione per l'accesso. Come buona pratica, assegnare l'autorizzazione per l'accesso al gruppo principale di tutti gli utenti di Configuration Manager.
- ➤ Questa soluzione si applica anche in casi in cui l'accesso non riesce quando proviene da un accesso al sistema IDM.

Problema. Il server Configuration Manager non si avvia perché sono state inserite credenziali del database non corrette.

Soluzione. Se si apportano modifiche alle credenziali del database e il server non si avvia, le credenziali potrebbero essere errate. (**Nota**: la Procedura guidata post installazione non esegue automaticamente il test delle credenziali immesse. È necessario fare clic sul pulsante **Test** nella procedura guidata.) È necessario crittografare nuovamente la password del database e immettere le nuove credenziali nel file di configurazione. Procedere come segue:

1. Da una riga di comando, eseguire questo comando per crittografare la password del database aggiornata:

   <directory di installazioneConfiguration Manager >\bin\encrypt-password.bat –p <password>

restituisce una password crittografata.

2 Copiare la password crittografata (incluso il prefisso {ENCRYPTED}), nel parametro **db.password** nella <**directory di installazione di Configuration Manager**>**\conf\database.properties**.

Problema. Se il DNS non è stato configurato correttamente, potrebbe essere necessario accedere utilizzando l'indirizzo IP del server. Quando viene immesso l'indirizzo IP, si verifica un secondo errore DNS.

Soluzione. Sostituire nuovamente il nome del computer con l'indirizzo IP. Ad esempio:

Se si accede utilizzando il seguente indirizzo IP:
http://16.55.245.240:8180/cnc/

e si riceve un indirizzo con il nome del computer che mostra un errore DNS, ad esempio:
http://my.example.com:8180/bsf/secure/authenicationPointURL.jsp...

sostituirlo con: http://10.0.0.1:8180/bsf/secure/authenicationPointURL.jsp...

e avviare nuovamente l'applicazione nel browser.

Problema. Il server Tomcat Configuration Manager non si avvia.

Soluzione. Procedere con una una delle seguenti operazioni:

- ➤ Eseguire la Procedura guidata di post installazione e sostituire le porte del server Configuration Manager.
- ➤ Interrompere gli altri processi che occupano le porte di Configuration Manager.
- ➤ Cambiare manualmente le porte nel file di configurazione di Configuration Manager modificando il seguente file: <**directory di installazione di Configuration Manager**>**\servers\server-0\conf\server.xml** e aggiornando le porte attinenti:
  - ➤ HTTP (8180): riga 69
  - ➤ HTTPS (8443): righe 71, 90

Problema. Viene visualizzato il messaggio "out of memory".

Soluzione. Procedere come segue per cambiare i parametri di avvio del server:

1 Eseguire il seguente file batch:

<directory di installazione di Configuration Manager>/bin/edit-server-0.bat

2 Cambiare le seguenti impostazioni:

-Dapplication.ms=<dimensione pool di memoria iniziale>
-Dapplication.mx=<dimensione pool di memoria massima>

Problema. La Procedura guidata di post installazione impiega molto tempo dopo aver fatto clic su **Finish**.

Soluzione. Per un sistema UCMDB che non è stato pre-configurato per la modalità consolidata, l'operazione di consolidamento dello schema può richiedere del tempo (in relazione alla quantità di dati). Attendere 15 minuti. Se non si rilevano progressi, interrompere la Procedura guidata di post installazione e riavviare il processo.

Problema. I cambiamenti nei CI in UCMDB non si riflettono in Configuration Manager.

Soluzione. Configuration Manager esegue un processo di analisi asincrona offline. Il processo potrebbe non avere ancora elaborato gli ultimi cambiamenti in UCMDB. Per risolvere il problema, provare una delle seguenti:

- ➤ Attendere alcuni minuti. L'intervallo predefinito tra le esecuzioni del processo di analisi è 10 minuti. Può essere configurato in **Sistema** > **Impostazioni**.
- ➤ Eseguire una chiamata JMX per eseguire il calcolo dell'analisi offline sulla vista pertinente.

- Selezionare **Amministrazione** > **Criteri** > **Criteri di configurazione**. Fare clic sul pulsante **Ricalcola analisi criteri**. In questo modo viene richiamato il processo di analisi offline per tutte le viste (può richiedere del tempo). È necessario inoltre apportare delle finte modifiche a uno dei criteri e salvarlo.

Problema. Facendo clic su **Amministrazione** > **UCMDB Foundation**, si apre la pagina di accesso di UCMDB.

Soluzione. Per poter accedere a UCMDB senza accedere nuovamente, è necessario abilitare single sign-on (SSO). Per informazioni, consultare "Single Sign-On (SSO)" a pagina 76. Inoltre, assicurarsi che l'utente di Configuration Manager che ha eseguito l'accesso sia definito nel sistema di gestione utenti di UCMDB.

Problema. Durante la configurazione di una connessione UCMDB nella Procedura guidata post installazione su un indirizzo IPv6, l'elemento del menu **Amministrazione** > **UCMDB Foundation** non funziona.

Soluzione. Procedere come segue:

1. Selezionare **Sistema** > **Impostazioni** > **Integrazioni** > **UCMDB Foundation** > **UCMDB Foundation.**
2. Aggiungere le parentesi quadrate all'indirizzo IP nell'URL di accesso a UCMDB. L'URL deve avere il seguente aspetto: http://[x:x:x:x:x:x:x:x]:8080/.
3. Salvare il set di configurazione e attivarlo.
4. Riavviare Configuration Manager.

LW-SSO - Risoluzione dei problemi e limitazioni

Problemi noti

In questa sezione vengono descritti i problemi noti per l'autenticazione LW-SSO.

- **Contesto di protezione.** Il contesto di protezione LW-SSO supporta un solo valore attributo per nome attributo.

  Quindi, quando un token SAML2 invia più di un valore per lo stesso nome attributo, solo un valore viene accettato dal framework LW-SSO.

  In modo analogo, se il token IdM è configurato per inviare più di un valore per lo stesso nome attributo, solo un valore viene accettato dal framework LW-SSO.

- **Funzionalità di disconnessione multi-dominio con Internet Explorer 7**. La funzionalità di disconnessione multi-dominio non va a buon fine nelle seguenti condizioni:

  - Il browser utilizzato è Internet Explorer 7 e l'applicazione richiama più di tre verbi redirect HTTP 302 consecutivi nella procedura di disconnessione.

  In questo caso, Internet Explorer 7 può non gestire correttamente la risposta redirect HTTP 302 e visualizzare una pagina di errore con il messaggio **Impossibile visualizzare la pagina Web**.

  Per ovviare al problema, si consiglia se possibile di ridurre il numero di comandi di redirect applicazione nella sequenza di disconnessione.

Limitazioni

Notare le seguenti limitazioni quando si lavora con l'autenticazione LW-SSO:

- **Accesso client all'applicazione**.

  Se nella configurazione LW-SSO è definito un dominio:

  - I client applicazione devono accedere all'applicazione con un nome dominio completo (FQDN) nell'URL di accesso, ad esempio, http://myserver.**companydomain**.com/WebApp.
  - LW-SSO non può supportare URL con un indirizzo IP, ad esempio, http://192.168.12.13/WebApp.
  - LW-SSO non può supportare URL senza un dominio, ad esempio, http://myserver/WebApp.

  Se nella configurazione LW-SSO non è definito un dominio: Il client può accedere all'applicazione senza un FQDN nell'URL di accesso. In questo caso, viene creato un cookie della sessione LW-SSO specifico per un singolo computer senza informazioni sul dominio. Quindi, il cookie non è delegato da browser a un altro, e non passa ad altri computer posizionati nello stesso dominio DNS. Questo significa che LW-SSO non funziona nello stesso dominio.

- **Integrazione framework LW-SSO.** Le applicazioni possono sfruttare e utilizzare le funzionalità LW-SSO solo se integrate precedentemente nel framework LW-SSO.

- **Supporto multi-dominio**.

  - La funzionalità multi-dominio si basa sul riferimento HTTP. L'W-SSO supporta pertanto collegamenti da un'applicazione all'altra e non supporta la digitazione di un URL in una finestra del browser, a meno che le due applicazioni non risiedano nello stesso dominio.
  - Il primo collegamento interdominio che utilizza **HTTP POST** non è supportato.

La funzionalità multi-dominio non supporta la prima richiesta **HTTP POST** verso una seconda applicazione (è supportata solo la richiesta **HTTP GET**). Ad esempio, se l'applicazione ha un collegamento HTTP verso una seconda applicazione, è supportata una richiesta **HTTP GET**, ma non è supportata una richiesta **HTTP FORM**. Tutte le richieste dopo la prima possono essere **HTTP POST** o **HTTP GET**.

- Dimensione token LW-SSO:

  La dimensione delle informazioni che LW-SSO può trasferire da un'applicazione in un dominio a un'altra applicazione in un altro dominio è limitata a 15 gruppi/ruoli/attributi (notare che ciascun elemento può essere lungo in media di 15 caratteri).

- Collegamento da pagine protette (HTTPS) a pagine non protette (HTTP) in uno scenario multi-dominio:

  La funzionalità multi-dominio non è utilizzabile nel collegamento da una pagina protetta (HTTPS) a una pagina non protetta (HTTP). È una limitazione del browser in cui l'intestazione di riferimento non viene inviata durante il collegamento da un risorsa protetta ad una non protetta. Per un esempio, consultare:
  http://support.microsoft.com/support/kb/articles/Q178/0/66.ASP

- **Token SAML2.**

  - La funzionalità di disconnessione non è supportata quando è utilizzato il token SAML2.

    Quindi, se il token SAML2 è utilizzato per accedere a una seconda applicazione, l'utente che si disconnette dalla prima applicazione non viene disconnesso dalla seconda applicazione.

  - La scadenza del token SAML2 non viene presa dalla gestione della sessione dell'applicazione.

    Quindi, se il token SAML2 è utilizzato per accedere a una seconda applicazione, la gestione della sessione di ciascuna applicazione è gestita indipendentemente.

- **JAAS Realm.** Il JAAS Realm in Tomcat non è supportato.

- **Uso degli spazi nelle directory Tomcat.** L'uso degli spazi nelle directory Tomcat non è supportato.

Non è possibile utilizzare LW-SSO quando un percorso (cartelle) di installazione Tomcat include gli spazi (ad esempio, File di programma) e il file di configurazione LW-SSO è posizionato nella cartella Tomcat **common\classes**.

- **Configurazione del bilanciamento del carico.** Si deve configurare un bilanciamento del carico distribuito con LW-SSO per poter utilizzare sessioni sticky.

Risoluzione dei problemi

Problema: Dopo l'accesso non viene creato un cookie LW-SSO.

- **Cause possibili:** È stato definito in modo non adeguato un dominio non vuoto nell'elemento LW-SSO della configurazione.
- **Soluzioni possibili**: Verificare che il dominio definito nell'elemento LW-SSO della configurazione sia uguale al dominio dell'applicazione.
- **Cause possibili:** Un dominio non vuoto passato come paramentro alla funzione enableSSO non è corretto.
- **Soluzioni possibili**: Verificare che il dominio passato come paramentro alla funzione enableSSO sia uguale al dominio dell'applicazione.
- **Cause possibili:** Non è possibile accedere all'applicazione con un nome dominio completo (FQDN) nell'URL di accesso quando un dominio è definito nella configurazione LW-SSO (ad esempio: http://192.168.12.13/WebApp).
- **Soluzioni possibili**: Verificare di accedere all'applicazione con un nome dominio completo (FQDN) nell'URL di accesso (ad esempio: http://myserver.companydomain.com/WebApp).

Problema: LW-SSO non è riuscito a creare un cookie per la funzionalità AutoCookieCreation.

- **Cause possibili:** Non è stato definito in modo adeguato un dominio nell'elemento LW-SSO della configurazione.
- **Soluzioni possibili**: Verificare che il dominio definito nell'elemento LW-SSO della configurazione sia uguale al dominio dell'applicazione.

Problema: Il token LW-SSO non è stato convalidato.

- **Cause possibili:** Le due applicazioni hanno diversi parametri initString nell'elemento crypto della configurazione (o altri parametri crypto).
- **Soluzioni possibili**: Utilizzare la stessa initString in entrambe le applicazioni (oltre a tutti gli altri parametri crypto nell'elemento di creazione di LW-SSO).
- **Cause possibili:** La differenza dell'orario GMT tra le due applicazioni è superiore a 15 minuti.
- **Soluzioni possibili**: Verificare che tutte le applicazioni comprese in una integrazione LW-SSO utilizzino lo stesso orario GMT con una differenza massima di 15 minuti.
- **Cause possibili:** Un dominio nell'elemento LW-SSO della configurazione è vuoto e si accede a una seconda applicazione su un altro computer con lo stesso dominio DNS.
- **Soluzioni possibili**: Verificare che il dominio definito nell'elemento LW-SSO della configurazione sia uguale al dominio dell'applicazione.
- **Cause possibili:** Non è definito un dominio nell'elemento LW-SSO della configurazione e si accede a una seconda applicazione su un altro computer con lo stesso dominio DNS.
- **Soluzioni possibili**: Aggiungere un dominio all'elemento LW-SSO e verificare che il dominio definito sia identico al dominio dell'applicazione.

Problema: LW-SSO non è in grado di convalidare il token LW-SSO in un ambiente multi dominio

- **Cause possibili:** Nella configurazione di una delle applicazioni, è stato definito in modo non adeguato un dominio nell'elemento LW-SSO.
- **Soluzioni possibili**: Il dominio definito nell'elemento LW-SSO della configurazione dell'applicazione deve essere lo stesso dominio dell'applicazione in base ai domini in uso.
- **Cause possibili:** Nella configurazione di una delle applicazioni, un dominio è definito in modo non corretto nelle impostazioni trustedHosts (o impostazioni protectedDomains).

- **Soluzioni possibili**: Verificare che i domini nelle impostazioni trustedHosts (o impostazioni protectedDomains) di tutte le configurazioni delle applicazioni siano definiti correttamente.
- **Cause possibili:** Il cookie della sessione LW-SSO è bloccato o negato quando si utilizza Internet Explorer 6.x, 7.x, o 8.x.
- **Soluzioni possibili**: Aggiungere tutti i server LW-SSO all'area "Intranet"/"Attendibili" nelle aree di protezione Internet Explorer sul computer (Strumenti > Opzioni Internet > Protezione > Intranet locale > Siti > Avanzate). In questo modo tutti i cookie saranno accettati.
- **Cause possibili:** Alcune applicazioni hanno diversi parametri initString nell'elemento crypto della configurazione (o altri parametri crypto).
- **Soluzioni possibili**: Utilizzare la stessa initString in tutte le applicazioni (oltre a tutti gli altri parametri crypto nell'elemento di creazione di LW-SSO).
- **Cause possibili:** La differenza dell'orario GMT tra alcune applicazioni è superiore a 15 minuti.
- **Soluzioni possibili**: Verificare che tutte le applicazioni comprese in una integrazione LW-SSO utilizzino lo stesso orario GMT con una differenza massima di 15 minuti.
- **Cause possibili:** Un collegamento multi dominio va da una risorsa protetta (HTTPS) ad una non protetta (HTTP).
- **Soluzioni possibili**: Quando si collega o si passa da un dominio all'altro, verificare che la prima richiesta di collegamento/passaggio vada da una risorsa protetta (HTTPS) ad una risorsa non protetta (HTTPS).

Supporto IPv6 - Risoluzione dei problemi e limitazioni

Limitazioni

- L'URL non può contenere un indirizzo IP.
- Il sistema operativo deve supportare sia IPv6 che IPv4. Non sarà possibile accedere al server Configuration Manager se l'indirizzo IPv4 non è chiuso o non è supportato.
- Tutte le volte che viene cambiato l'orario sul server Tomcat di Configuration Manager, il server deve essere riavviato per poter aggiornare l'ora sul server.

Risoluzione dei problemi

Problema. Una volta configurata una connessione di UCMDB a un indirizzo IPv6 durante l'installazione, l'opzione del menu **Amministrazione** > **UCMDB Foundation** non funziona.

Soluzione. Procedere come segue:

1. Selezionare **Sistema** > **Impostazioni** > **Integrazioni** > **UCMDB Foundation** > **UCMDB Foundation.**
2. Aggiungere le parentesi quadrate all'indirizzo IP nell'URL di accesso al campo UCMDB. L'URL deve avere il seguente aspetto: http://[x:x:x:x:x:x:x:x]:8080/ucmdb-ui/.
3. Salvare il set di configurazione e attivarlo.
4. Riavviare Configuration Manager.

Autenticazione - Risoluzione dei problemi e limitazioni

Questa sezione descrive i problemi di autenticazione noti.

Problema: Durante l'autenticazione su un'applicazione dopo il reindirizzamento a un punto di autenticazione, si riceve l'errore 500.

- **Cause possibili:** WAR e BSF WAR di Configuration Manager hanno diversi parametri initString nell'elemento crypto della configurazione (o altri parametri crypto).
- **Soluzioni possibili:** Utilizzare la stessa initString in entrambe le applicazioni (oltre a tutti gli altri parametri crypto nell'elemento di creazione di LW-SSO).

Problema: Durante l'autenticazione su un'applicazione dopo il reindirizzamento a un punto di autenticazione, non viene visualizzato il modulo di accesso.

Soluzione: Il cookie della sessione di autenticazione di Configuration Manager è bloccato o rifiutato quando si utilizza Internet Explorer versione 6.0, 7.0 o 8.0. Aggiungere il server Configuration Manager all'area **Intranet/Attendibili** nelle aree di protezione di Internet Explorer sul computer (**Strumenti** > **Opzioni Internet** > **Protezione** > **Intranet locale** > **Siti** > **Avanzate**). In questo modo tutti i cookie saranno accettati.

Problema: Dopo l'autenticazione, si riceve l'errore 403.

- **Cause possibili:** Non è stato definito in modo adeguato un dominio nell'elemento LW-SSO della configurazione dell'applicazione.
- **Soluzioni possibili:** Verificare che il dominio definito nell'elemento LW-SSO della configurazione dell'applicazione sia uguale al dominio dell'applicazione.
- **Cause possibili:** Non è possibile accedere all'applicazione con un nome dominio completo (FQDN) nell'URL di accesso quando un dominio è definito nella configurazione LW-SSO (ad esempio: http://192.168.12.13/WebApp).
- **Soluzioni possibili:** Verificare di accedere all'applicazione con un nome dominio completo (FQDN) nell'URL di accesso (ad esempio: http://myserver.companydomain.com/WebApp).

Problema: Dopo l'autenticazione, viene visualizzata la pagina **Ottieni dettagli utente Acegi**.

Soluzione: Il cookie della sessione di autenticazione di Configuration Manager è bloccato o rifiutato quando si utilizza Internet Explorer versione 6.0, 7.0 o 8.0. Aggiungere il server Configuration Manager all'area **Intranet/Attendibili** nelle aree di protezione di Internet Explorer sul computer (**Strumenti** > **Opzioni Internet** > **Protezione** > **Intranet locale** > **Siti** > **Avanzate**). In questo modo tutti i cookie saranno accettati.